Security and collaborative groupware tools usage

By
Resala A. AlAdraj

A thesis submitted in partial fulfillment of the requirements for the degree
of
Doctor of Philosophy in Computer Science

University of Warwick, Department of Computer Science
June, 2015

Acknowledgement

I would like to take this opportunity to thank all who have supported me during the PhD study. Special thanks to my first supervisor, Dr.Mike Joy, for his encouragement, supervision and support from the preliminary to the concluding level which enable me to understanding of the subject. In addition to that, I would like to thank my co-supervisors, Dr. Matthew Leeke and Dr. Alexandra Cristea for their suggestions and feedback made to this thesis.

I am extremely thankful for Dr. Jonathan Foss for his critical proof reading. I am heartily thankful to Prof. Khalil Alkhalili, Vice Director of Scientific Publishing Center at the University of Bahrain who coached and guided me in statistical analysis and presentation during my study. I am most grateful for his tireless support.

Many thanks to Dr.Hesham Al-Ammal, Dean of IT College, Dr. Ali Zolait, Editor-in-Chief: International Journal of Technology Diffusion (IJTD) in the University of Bahrain for their advice and evaluating my survey. Also special thanks for Dr. Ahmed AlMasri from the Arab Open University for his help during distribution of the survey.

Further thanks to Dr.Fareed Bayat from Art College at the University of Bahrain for his continued guidance during my study.

Special thanks goes for my husband Yaser AlRayyes for his support, valuable advices and provided me with absolute freedom during my study.

Dedication

To the soul of my parents, my younger sister, my eldest brother.

I would also like to dedicate this study to my husband, daughter and son for their patience and support in spirit which helped me undergo this program of study.

Table of contents

List of Figures

List of Tables

Abstract

This thesis investigates the usage problems of Online Collaborative Groupware (OCG) tools for learning at the University of Bahrain (UOB) in the Kingdom of Bahrain. An initial study revealed that the main problems faced by students when they use OCG tools in the learning process are security and trust.

SWFG (Skype, Wiki, Facebook, and Gmail) tools were proposed as being effective and commonly used OCG tools for learning. A quasi-experiment has been done with UOB students to identify the perceptions of the students towards security, privacy and safety relating to use of SWFG tools. Based on this experiment the researcher has derived the following results:

- Secure Skype has a positive relationship with Skype usage;
- Private Skype has a positive relationship with Skype trust;
- Secure Gmail has a negative relationship with Gmail usage and trust;
- Wiki usage has a negative relationship with trust in Wikis.

Additionally, the research revealed that students may be more motivated to use OCG tools if the security and privacy of these tools was to be improved. The thesis also focuses on security and trust within email.

In order to evaluate the usage of secure emails, students' awareness of the secure email awareness was investigated using quantitative and qualitative methods. The results of this evaluation informed the design of an experiment that was then conducted by tracking secure email usage and gathering information about the students' usage and awareness of their secure emails. The aim of this activity was to identify a clear representation of secure email usage over specified periods for both academic and non-

academic purposes by students in both the UK and Bahrain. It has been concluded from this experiment that there are differences between the usage of secure email in each country when applied to both academic and non-academic purposes.

Finally, based on these results, the researcher developed a framework which derives from the Technology Acceptance Model (TAM) model by testing security and trust effects on the ease of use and on usefulness. A case study has been conducted using a new secure email instructional model in order to validate the research framework. The study found that security provided by webmails and students' trust affects the webmail's perceived usefulness, and that in turn this leads to ease of use regardless of which type of email client is used. However, it was not proof that usefulness affects the usage of email. Evidence suggests that the model may be a suitable solution for increasing the usefulness of email in Computer Supported Collaborative Learning (CSCL), and can help to strengthen communication between faculty and students.

This study has contributed valuable knowledge and information in this particular field of study. It has been able to gather a satisfactory amount of information from both students and teachers in both the University of Bahrain (UOB) and the University of Warwick (UOW). A number of different methods were used in this task – interviews, questionnaires, observations, experiments and student feedback, amongst others.

The entire study was conducted in a way that it would empirically evaluate different dimensions of secure Online Collaborative Groupware (OCG) tools usage in the educational environment. The research framework applied in this investigation provided many insights into OCG tools. These new insights and information may be used to test and validate the framework with a large number of students.

Abbreviations

UOW	University of Warwick
UOB	University of Bahrain
TAM	Technology Acceptance Model
IT	Information Technology
IS	Information System
SWFG	Skype, Wikipedia, Facebook, and Gmail
CSCL	Computer Supported Collaborative Learning
OCG	Online Collaborative Groupware
SSPT	Security, Safety, Privacy, and Trust
VLE	Virtual Learning Environment
LMS	Learning Management Systems
PEOU	Perceived Ease Of Use
PU	Perceived Usage
PII	Personally Identifiable Information
HTTPS	HyperText Transfer Protocol
HSSRE	Human and Social Science Research Ethics Committee
WYSIWYG	What You see Is What You Get
UOC	Universitat Oberta de Catalunya

Chapter One: Introduction

1.1 Introduction

The web has changed from a simple hypertextual repository of documents to a powerful communication medium. This change has caused educational activities to be supported by web applications, which often include collaborative sessions. A wide range of technologies has been prepared by educational institutions in order to support collaboration between learners, and also between learners and teachers. In recent years, web-based technologies have allowed people who are located in different places to interact with each other in synchronous and asynchronous ways. These technologies provide significant potential for supporting collaborative learning activities. Collaborative groupware can broadly be defined as a process of learning in which two or more people learn something together.

Discovery of the right tools to support groupware, and intensive use of technology that supports certain activities (such as chatting, messaging, and documents sharing) should support students with learning, in order to ensure a successful educational process.

The ubiquity of the Internet and online technologies provides a framework within which Online Collaborative Groupware (OCG) tools such as Skype, Wikipedia, Facebook and Gmail (SWFG) become widely available and provide benefits for student learning. Since portable devices can access e-learning systems anytime and anywhere, there are challenges facing the usage of OCG tools, relating to students' concerns about the usage of OCG tools. In particular, one of the biggest challenges is security and trust.

1.2 A profile of UOB

1.2.1 Introduction to Bahrain

Bahrain comprises an archipelago of 33 islands in the Arabian Gulf, situated close to the shore of the Arabian Peninsula. The islands are about 24 kilometres from the east coast of Saudi Arabia and 28 kilometres from Qatar.

Figure 1.1:Bahrain's location (Travellerpoint, 2014)

Figure 1.2: Bahrain map (Travellerpoint, 2014)

Recently, there are four public universities and higher education institutions such as UOB, and 19 private universities and higher education institutions such as Arab Open University (AOU) (Travellerpoint, 2014).

1.2.2 Introduction to UOB

The University of Bahrain (UOB) is the only national higher education institution in the

Kingdom of Bahrain that offers mainly undergraduate Bachelor degrees and some postgraduate degrees. It was founded in 1986. Its roots date back to the late sixties when two higher education institutes were founded, namely the Higher Institute for Teachers and the Gulf Technical College. The students' population during Semester 1, 2012/2013 was 18,137 (Female 68%, Male 32%).

Recently the university has the following mend:

- PhD 7 theses were produced;
- 4 Sports Management College of Education (currently the college of Physical Education and Physiotherapy) and,
- 3 College of Engineering (2 Electrical, 1 Mechanical) (UOB, 2012).

The University of Bahrain now comprises nine colleges:

- College of Arts.
- College of Business Administration.
- College of Education.
- College of Information Technology.
- College of Law.
- College of Science.
- College of Engineering.
- College of Applied Studies.
- Bahrain Teachers' College.

Ranking of the University:

Webometrics: 1st at local universities level, 40 at Arab Universities level, and 2841 at International level in July 2012 (out of 17,000 universities).

1.2.3 Introduction to IT College

The College of Information Technology was established in 2003 to contribute to the success of the University of Bahrain's mission of excellence in learning, knowledge creation and transfer and engaging society within the IT and computing disciplines. The college programs in Computer Science, Computer Engineering, and Information Systems have all been accredited by ABET. Furthermore, the College offers an MSc programme in Computing. We recognize clearly that the role of the national university in achieving Vision 2030 and contributing to the Kingdom's participation in the knowledge society depends on having a strong infrastructure and capacity in IT (ALAmmal, 2014).

1.3 Choice of Topic

The research includes an investigation into the Online Collaborative Groupware (OCG) tool usage in learning. This PhD research has been undertaken in combination with her role as a lecturer at the IT college at the University of Bahrain (UOB) in that the areas investigated in this study can support face-to-face teaching, which would subsequently enhance the learning and teaching in UOB.

The OCG considered in this study are undergoing rapid evolution, and require the emergence of new concepts for their effective use in teaching and learning.

1.4 Problem Statement

From the author's experience, in twenty years of teaching, and also after speaking to colleagues who work in the same field, it has become clear that the number of students who are studying in UOB is increasing and there is a lack of communication between teachers and students. Moreover, UOB students are not up-to-date with educational technology tools and this leads to restricting the students into face-to-face meetings

which waste the teachers' time. In addition to that the students and teachers are not feeling comfortable and enjoying these tools as they think that these tools have a lack of security. In other words they think that these tools expose users easily to hackers. Moreover, the students feel tense during assignment submission as they also think their assignments may be exposed to hackers.

1.5 Thesis Outline

This Chapter will discuss the aim and objectives of this research. The main background of the study will be introduced, and all the appropriate issues with the OCG tools usage will also be discussed.

Chapter 2 presents the summary of the literature review.

Chapter 3 discusses the research methodology used in this study.

Chapter 4 discusses the triangulation methods undertaken in order to determine the difficulties and problems faced by UOB students and teachers when using OCG tools.

Chapter 5 evaluates the security, safety, privacy and trust of the SWFG tools by conducting a quasi-experiment with UOB students.

Chapter 6 investigates the awareness of the secure email usage using a triangulation method.

Chapter 7 presents a secure email tracking intervention.

Chapter 8 validates the research framework by conducting a case study with UOB students.

Finally, Chapter 9 delivers the discussion, conclusion and recommendations. Additionally, Chapter 9 also presents ideas for future work.

1.6 Background to the study

The study is based on the initial study that was conducted as part of the overall study, and this was comprised of:

1. Student questionnaire.
2. Teacher interviews.

Ethical consent was obtained for this research using the procedures delegated to the Department of Computer Science by the Human and Social Science Research Ethics Committee (HSSREC) in the University of Warwick.

This initial study was essential to determine the initial point for the PhD study in terms of the difficulties and problems faced by students in using OCG tools in learning. The initial study has investigation in the form of a questionnaire and interviews applied to Information system (IS) students and faculties in the University of Bahrain (UOB). This will be discussed in Chapter 4 of this study.

The results of the student questionnaires indicated that the major problems with the usage of OCG tools are the "trust" and the "students' awareness of secure OCG tools".

The results of the interviews held with seven teachers indicated that:

- IT lecturers have to manage large classes and it may be difficult to pay individual attention to students.
- Students have a lack of motivation to use OCG tools due to the lack of trust.
- Teachers do not use learning technology, such as emails, Facebook, or any other modern OCG tools.
- The teachers rely on conventional media forms, including books, notes, PowerPoint, for convenience.

These findings confirm the problems indicated in Section 1.3, above, and the need for new technology and methods to support conventional teaching-learning methods. The author, in this context, proposes that in order for teaching/learning to be purposeful and effective for the benefit of the students, it must be based on a combination of face-to-

face class room based lectures, that are augmented with e-learning resources that involve OCG tools such as Facebook, Twitter, Emails, and Skype.

For the purpose of this research, the researcher has adapted definitions for the following terms.

- Security means that information shared by the tool will only be accessible to those for whom it is intended.

- Secure OCG tools have been defined for the purpose of this research as OCG tools that have the tools' security settings enabled.

- Private OCG tools have the ability for students to isolate information about themselves and thereby reveal themselves selectively.

- Safe OCG tools are protected from harm such as viruses, spyware, etc."

- Trust is a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another." (Rousseau, 1998).

- Trusted OCG tools are tools that the students feel relax and at ease when using.

Using these definitions, the research questions and hypotheses will be discussed later in this Chapter.

1.7 Aims and Objectives

1.7.1 Aim

The aim of this research is to produce an innovative instructional secure OCG framework for effective OCG tools usage to support teaching and learning in UOB.

1.7.2 Specific Objectives

The main motivation of this research is to solve the problems faced by the students and teacher when using OCG tools, as discussed in Section 1.3. In doing so, the main objectives of this study are:

1. to investigate the current extent to which OCG tools are used and to identify the students' perceptions towards OCG tools in UOB;
2. to investigate how secured OCG tools would enhance student usage and trust of OCG tools;
3. to evaluate secure email awareness in order to propose and evaluate a framework that describes secure email usage.

1.8 Research Questions

The main research questions are as follows:

In conducting this study the researcher has developed four main research questions as follows:

1. What is the perception of students towards security, privacy, and trust when using OCG tools during the learning activities?
2. Are students aware of secure email usage and how often do they access their emails for academic purposes?
3. Does Secured and trusted emails lead "ease of use" and "usefulness" ?
4. Does "ease of use" and "usefulness" lead to email usage?

These research questions will lead to more detailed research questions which will be addressed in the individual Chapters.

1.9 Research Hypotheses

Hypothesis 1:

H1: There are significant correlations between security, trust, privacy and safety of OCG tools and their usage.

Hypothesis 2:

H2: Students are aware of secure email.

Hypothesis 3:

H3: Secured and trusted emails lead to "ease of use" and "usefulness".

Hypothesis 4:

H4: "Ease of use" and "usefulness" leads to an increased usage of emails.

1.10 Research Methodology

The research methodology for this study is discussed in detail in Chapter 3. However, it can be summarized as follows:

1. A literature review into areas related to teaching and learning in collaborative groupware. This includes e-learning and educational technology, social networking media, with specific emphasis on how the security and trust concepts are applied to OCG tools.

2. Investigation of the students' perception towards secure OCG tools such as Skype, Wikis, Facebook, and Gmail (SWFG) by conducting a quasi-experiment with UOB students, using a triangulation method by developing a SWFG usage model.

3. Evaluation of the students' awareness of secure email by using a triangulation method to compare the UK and UOB students

4. Tracking the students' usage of secure emails by using an email tracking form for

academic and non-academic purposes with the UK and UOB students.

5. The development of an instructional model for email usage within learning.

6. Validation of a secure email usage framework by conducting case studies with UOB students.

In this study, the researcher conducted data analysis using SPSS.

1.11 Expected study outcome

By the end of this study, it is expected that the research will have been able to:

- create a suitable instructional model for using OCG tools in the learning at UOB;
- validate the application of OCG tools at UOB;
- demonstrate the implementation of email usage at UOB.

1.12 Chapter Summary

In this Chapter, the problem statement along with the main aims and objectives of this study have been presented. The Chapter has also outlined the scope and limitations of this proposed study. The main background of the study has been introduced in this Chapter, and all the appropriate difficulties and problems faced by students in using OCG tools in learning in UOB have also been discussed. Finally, the Chapter also provided a brief introduction to Bahrain and UOB which is the focus of the study.

Chapter Two: Literature Review

2.1 Introduction

This Chapter provides an overview of an examination of published papers defining contemporary research relevant to the research topic discussed in Chapter 1. The Chapter cites literature from several areas to cover the technical aspects of the educational part of collaborative groupware learning activities, OCG tools and the security concerning this research. A critical review of the literature identifies the questions that are the basis for this research.

This Chapter contains four main Sections. The first, Section 2.2, defines technological approaches for supporting learning. The next three sections address each of the research questions through reviews of published papers relating to OCG tools, especially in education and security. From this critical review, the high-level research questions are identified which will be discussed in Chapter 3.

2.2 Technological approaches to supporting learning

Technology in the classroom has become a major trend in teaching and learning especially at the college level; such a situation therefore needs to be clearly discussed. The details of relevant technology are educational technology, e-learning, virtual learning, and social networking sites.

2.2.1 Educational Technology

Trinidad (2003) claimed that "Technology-rich learning environments can engage the learner giving them a sense of empowerment, in which they work in a community of learners that is guided by teachers or instructors, instead of depending on these

educators, who might not have such a broad knowledge of a particular subject." In other words, students can contribute to the procedure of pedagogical revolution that includes real-world presentation of new resources, latest techniques and novel views. Simultaneously, by applying new e-learning technologies teachers will be able to shift their focus from teaching to learning.

Digital education environment produces opportunities for creating an educational environment that improves the style of old environment and focuses on providing more information, optimizing the educational process and improving the effect of education. Students can pick the information by themselves which supports the practical ability of them (Zhengjun *et al* 2008). Therefore, students can be improved by applying the educational technology practice in their study work. Educational technologies include digital presentation of educational content, in which information is presented using images, animation, and virtual environment.

Zhengjun *et al* (2008) also commented that the digital educational environment can create opportunities for personal teaching, which makes students more active, and inspires their potential abilities.

However, Keengwe *et al* (2008:39) argued that the educators today are faced with many new challenges and responsibilities which is utilizing technology resources to enhance student learning. They highlighted the US Department of Education (2002) report which stated "Teachers must be comfortable with technology, able to apply it appropriately, and conversant with new technology tools, resources, and approaches." If all the pieces are put into place, teachers should find they are empowered to advance their own professional skills through these tools as well.

It is important to consider matching suitable and appropriate technology with content,

because use of technologies can provide the students with a more interesting and enriching experience, thus making them more prepared for the demands of the workplace. Bear in mind the students who do not like to use technologies in learning, those students have to be motivated and encouraged to use the most convenient technology that suits them.

2.2.2 E-Learning

E-Learning integrates technologies new knowledge to allow learners to learn at anytime and anywhere without constraints of time and space. E-learning has had a dramatic increase recently, and many educational institutions operators have released their own instructions based on E-Learning methods, including CD or cassette-based distance learning, single-learner online learning, and multi-learner multimedia-assisted instructions (Ching-Hong, 2010).

2.2.3 Virtual Learning Environment

The main purpose of Virtual Learning Environments (VLEs) is to engage students in the learning process by providing flexibility in where and when this process takes place. A key component of a virtual classroom is communication among students, and between students and their teachers, for which use can be made of tools such as e-mail, discussion groups and notice boards. Other important functions of VLEs are the delivery of learning resources, and the assessment and tracking of students (Suleman, 2003).

Indeed, in my opinion, different media, flexible time and space factors can be utilised to promote learning. In other words, VLEs make students' contributions more practical as they can develop communication tools asynchronously, access materials, interact with teachers or colleagues, and offer their contributions at whatever time suits them. Online discussion forums can also encourage active learning in that projects can also be

accessed in a virtual environment, facilitating peer review and collaboration at times and in places that suit the students outside the traditional classroom space.

I argue that a VLE has these advantages in some situations, especially in UOB classes. Indeed, this kind of VLE is not reliable and applicable in most departments. The students are dependent on their teachers and they prefer face to face learning and they are discouraged by their teachers fro using on line tools.

However, e-learning has many disadvantages. One of them is isolation in the online classes. Often, because the online classes are flexible, the student may be the only one in the online class. If there is no online interaction the student may feel bored and then prefers the real class as interacting with fellow students helps them to interact with the course and materials.

I addition to that, information reliability is another disadvantage and may affect the students' contented. Andrew (2003) clarifies that "although online materials usage are cost effective in that printing costs are often passed on to the student, students are often not able to determine the reliability of information, which can have a negative result on their studies". Educators must overcome this problem by keeping themselves up-to-date with what is happening on the website. However, this is a time-consuming task and extra to their other duties.

2.2.4 Social Media Sites

Treepuech (2011) defined Social Networking as "a social or gathering which creates the relationship among groups of people who appear on the Internet as an online community." This statement is important because it provides us with a clear definition, and this technology can permit people to meet, exchange thoughts, share experiences together, and collaborate in different ways.

Nowadays, Social Networking Sites (SNSs) have been growing in use. Information

technology helps ease a social networking site's access and the SNSs have significant functionality, so the number of users has been increasing dramatically in a very short time.

Facebook, Twitter, and Google Plus are among the most common SNSs. SNSs have an increasing significance in the society and people are spending more time on these services. Consequently, "the application of SNSs has been seen in various aspects such as telecommunication, marketing, education, entertainment, or even political. SNSs might not be able to serve all needs for every intention; however, SNSs may be able to support the operation to some extent, such as for promotion, for communication with target audiences, for making appointment, for sharing something that you want" (Treepuech, 2011).

Facebook, Twitter, Wikis and YouTube can be used as tools in education for sharing collaboration and posting comments. The trend and direction of utilising such SNSs leads to the development of teaching and learning management. Consequently, the student has more satisfaction with the teaching and learning management by SNSs than by traditional LMSs (Learning Management Systems) even though the teaching and learning management by SNSs is suitable for a limited group of students.

Thus, technological development in the internet and the possible combinations of SNSs in education, contributes effectively in the application of collaborative learning providing students with the opportunity to work in groups instantaneously, on the same intelligent environment, as Tsoulis *et al* (2013) stated "both in the same classroom and between cooperating schools, irrespectively of location". The application of Computer Supported Collaborative Learning (CSCL) models in the classroom requires the reshaping of existing traditional structures and the roles of protagonists. Both teachers and students participated in this process sharing different roles and responsibilities

(Finkel and Monk 1983) cited in (Tsoulis et al, 2013). A number of studies are focused on the benefits for learners that are involved in processes of collaborative construction of knowledge (Ertl, *et al*, 2006; Lou, *et al*, 2001) cited in (Tsoulis *et al*, 2013) have conducted research to answer the following research questions.

- Can we utilize effectively CSCL in primary education?
- What is the gain of CSCL application in primary education and what factors inhibit it?
- Is the interface of the educational software or the collaborative method applied by the teacher the essential factor for effective learning?

"Educational environments, which are free on the Internet, combined with successful management of students by the teacher, can achieve an effective collaborative learning process that can change the traditional teachers' and students' roles catalytically giving a new dynamic in contemporary education" (Tsoulis *et al*, 2013). CSCL to be success it must first dependant on the skills, enthusiasm and attitude of charismatic teacher. A teacher can utilise group dynamics in the classroom and the teacher can be a factor that can change the student to a modern explorer. It would seem that CSCL will utilise group dynamics of the classroom through the application of the appropriate educational situation which makes the student a contemporary researcher.

Nevertheless, Lederer (2012) lists some of SNSs problems such as:

- SNS can be a distraction tool, taking students' attention away from what is happening in class, and are ultimately disruptive to the learning process;
- Cyberbullying – while social networking sites provide a way for students and teachers to connect, they can be a weapon of malicious behaviour even on college campuses;
- Discouraging face-to-face communication.

In addition to these problems, the security of the educators' personal data and information is a major problem of the SNSs. This will be detailed later in this chapter.

2.2.5 Conclusion

As discussed so far, the effective use of technology can promote the process of learning, and is considered as a supportive additional tool for the educators towards enhancing learning outcomes, being specifically useful in teaching difficult aspects of subject areas. Students may face some problems that the technology can solve for them. In addition to that, it can be used as a motivation tool as it can make the learning more interesting and engaging.

Technology therefore provides a great opportunity to increase a student-centred attitude and reveal students to unlimited, verified and authentic knowledge and resources, rather than depending on what could be limited knowledge on the part of the instructors.

Nevertheless, to reach the best utilisation of technology in teaching requires particular conditions, including the level of awareness, which are matched by establishment of the correct tool, interactivity and training in the use of technology.

Therefore, the following aspects have been taken into consideration.

1. Interactions between the learning technology, teaching style and how it is used are complicated. Therefore, students' learning styles and their ability to use technology must be considered – both inside and outside the classroom.

2. Students' trust in the technology tools affects their motivation and learning. This can lead to an effective way of inspiring awareness in subjects that can be boring, or technically challenging.

2.3 Online Collaborative Groupware

OCG in education has become a major trend in teaching and learning especially at the college level; such situations therefore need to be clearly discussed. The following sections deal with this aspect.

2.3.1 Groupware

Groupware is defined in many different ways in the literature. Gutwin & Greenberg (1999) defined ccollaborative groupware as teaching tools that use multimedia, messaging and other social networks to facilitate communication between students and a teacher during interactive teaching.

Terpstra (2002) claimed that groupware is a software application and computer-based system designed for (or being used to) help groups of people and their communications and accomplishments as a group. Greenberg (2002) emphasised that groupware is software: "Groupware is software that supports and augments group work". Baker *et al* (2002) also mentioned in their paper groupware applications such as email, video conferencing, whiteboard, and GroupSketch which is a multi-user sketchpad running on a network.

Rouse (2005) pointed out "Groupware is often broken down into categories describing whether or not work group members collaborate in real time (synchronous groupware and asynchronous groupware)".

Indeed, the definition of Gutwin & Greenberg (1999) is somewhat inadequate because that definition does not cover the nature of groupware. In other words, is it software or hardware? Moreover this definition does not clarify that the users must be active simultaneously. In other words, it is not specified that groupware covers two types: real-

time groupware and non-real-time groupware. However, Terpstra (2002) has defined groupware clearly, Gutwin & Greenberg (1999) clarified the definition, and Rouse (2005) explains both categories of the groupware which are the main features of the groupware.

2.3.2 Online collaboration

"Collaboration is a relational system in which two or more stakeholders can share the resources together in order to meet objectives that could be met individually" (Graham & Barter, 1999) cited in (D'Agostino, 2013). They confirming the work of (Bill Bramwell, 2004) who clarify that "collaboration occurs when a group of autonomous stakeholders of a problem domain engage in an interactive process, using shared rules, norms, and structures to act or decide on issues related to that domain".

Web collaboration provides educational institutions with the capability to collaborate with students internally via the Internet in real-time. Those engaged in online collaboration can work together on office applications such as word processor documents and PowerPoint presentations, and even for brainstorming, without needing to be synchronous.

Software usability measures the ability of software to be attractive to a user, understood, learned and used under particular conditions. Gutwin & Greenberg (1999) both point out that groupware usability is "the degree to which a groupware system supports the activities of collaboration: communication, coordination, planning, monitoring and assistance".

Online collaborative groupware has some good features and some limitations, which are described and discussed below.

2.3.3 Advantages of collaboration groupware

There are many advantages of groupware, as expressed by Gunnlaugsdottir (2003). One of the main arguments in favour of groupware is the ability to facilitate internal and external communication with the addition of social networking tools such as electronic mail and messaging. Furthermore, the intranet can be used to post announcements and news to all particular groups "at the push of a button".

Another point in favour of groupware is that scheduling meetings can be done easily by using group calendaring and seeing when people are available or where they are. Another advantage is the opportunity for team members all over the world to collaborate and hold meetings online using video conferencing.

One further advantage is that using the records of information in the system can facilitate the design, capture, storage and retrieval of documents. Moreover, there is an opportunity for the necessary documents of the organization to be updated online, confirming that all employees are using the same and the latest version of the document. Furthermore, by using groupware, the information and knowledge is organized, indexed and can be shared; this prevents overloading of information and also prevents redundancy and re-invention. Additionally, experience and knowledge can be acquired from preceding assignments or projects. These practices will be available to those starting a new assignment or project. Ideas for new products or services can similarly be stored in an ideas bank (Marotta, 2006).

Further advantages, as stated by (Marotta, 2006) are that "groupware has characteristics such as efficiency and creativity. This means that during group work all the redundant work is eliminated, less time is spent searching the data, and more time is spent working on required tasks". The author also clarified that during group work, information can

easily be shared, and individuals can build on one another's information when collaboration is enabled.

2.3.4 Disadvantages of Groupware Systems

Despite the benefits of online groupware, there are also limitations. For example, the necessity for training users how to use the groupware tools may lead them to avoid using the system. Another disadvantage is interoperability, which refers to a situation in which users are involved in a groupware environment to meet each other in which collaboration groupware does not allow users to observe other's signals and facial expressions, and to hear voice inflections. (Stoy, 2010) echoes (Marotta, 2006) when he argues that groupware always relies on non-verbal communication. Any communication medium that does not provide for the use of non-verbal communication, such as facial expressions, gestures, etc., makes business communication more difficult and misunderstandings more common. These flaws may affect the efficiency of that technique.

Stoy (2010) also illustrates that many tasks are done more productively outside the groupware than inside it. Additionally, reliability could also be an issue with group collaboration software. A further disadvantage is that groupware costs a lot – especially for ordering, deploying and maintaining groupware software. Dependency on a software vendor affects the utilization of the groupware process and then leads to uninterested users and technicians. A further argument against groupware is the security and authentication. For instance, unauthorized access and risks can occur during transit of data.

2.3.5 OCG tools and education

The evolution of World Wide Web technologies since 1990 from Web 1.0 to Web 3.0

have dramatically influenced student learning, thus providing a new learning environment beyond those traditionally conducted. However, students in academic institutions, who are categorised as digital natives, are familiar in using Web 2.0 tools for their personal life but lack the primary skills to use them academically.

Danyaro *et al* (2010) commented "web 2.0 is increasingly becoming a familiar pedagogical tool in higher education, facilitating the process of teaching and learning. But this advancement in information technology has further triggered the problems like plagiarism and other academic misconduct". Danyaro *et al* (2010) concluded that " students use social websites for chatting, gamming and sharing files. Facebook, YouTube and Wikipedia are ranked as the most popular websites used by college students. They also revealed that students have an inherent desire to express ideas and opinions online openly and independently." This suggests this feeling of freedom makes students become more proficient, independent or participative and find learning to be less tiresome.

2.3.5.1 A Framework for Collaborative Learning System Based on Knowledge

Ruoman and Chuan (2009) described in their paper a framework for collaborative learning system that is based on knowledge management. They explained on their framework that communication tools are essential for the CSCL system as it is an efficient group collaborative learning environment and must provide some communication tools which satisfy the requirements of collaborative learning to exchange information, to coordinate actions and to reach agreements. These communication tools consist of Email, Wiki, Blog, BBS, Chat, Video Conference, etc.

2.3.5.2 Emotional Awareness in Collaborative Systems

Awareness is an essential issue, as it is an important characteristic of groupware systems

when compared with other multi-user systems. Collaboration awareness is the ability to convey information of other participant's presence and their role during collaboration. Indeed, awareness shows a critical role in collaborative work as Garcia *et al* (1999) clarified that "the users must know with whom they are working, but it can also be important to know where in the document they are at a particular moment, changes they have made to the shared workspace, and their area of influence, and their intentions."

2.3.5.3 Social Context for Computer-supported Collaborative Learning

Social context has an important role in interpersonal communications, which directly determines if the two parties can communicate and collaborate with honesty, trust, and openness. Bronfenbrenner (1979) cited in (Hart, 1993) depicted social context as "a pattern of activities, roles, and interpersonal relations experienced over time by the developing person with particular physical and material characteristics".

Learners, as social individuals need to frequently communicate and collaborate with teachers, peers, and experts to increase their knowledge and competence. Hernandez *et al* (2012) defined learning as a process of social negotiation or collaborative sense making, mentoring, and joint knowledge construction. According to (Dillenbourg, 1999) "collaborative learning is often defined as a situation in which two or more people learn or attempt to learn something together, and collaboration involves the mutual engagement of participants in a coordinated effort to solve problems together… CSCL is focused on how collaborative learning supported by technology that can enhance peer interaction and work in groups, and how collaboration and technology facilitate sharing and distributing of knowledge and expertise among community members".

2.3.5.4 OCG tools for Collaborative Writing Tools

Collaborative tools such as wikis, Skype, social media and emails can be used to facilitate CSCL tools in order to enhance learning. In addition, collaborative tools can enhance peer interaction and group work, facilitate sharing and distribute knowledge and information among a community of learners. (Lipponen, 2002) and (Cattafi & Metzner, 2007) cited in (Lipponen, 2002) claimed that "collaborative tools can serve as a knowledge platform for a community of practice where members of the community can share their knowledge with the group, post information, work together, and critically discuss issues".

They also commented that the "use of collaborative tools is characterized by some of the elements fundamental to a community of practice, including an online presence, a variety of interactions, communication, participation, relevant content, and relationships to a broader subject field of interest". Furthermore, the learner works as an essential element of collaborative learning. In other words, learners should be encouraged to reflect on their knowledge. Collaborative tools allow this reflection to be moved closer to a fully social constructivist mode of learning.

The following are some of the CSCL tools that can be used as collaborative writing tools:

A. Wikis and education

A Wikipedia is a web tool that allows users to easily create and edit web pages collaboratively (Strnad & Rugelj, 2010). A wiki may be described as a collaborative authoring tool. Wikipedia was created by Ward Cunningham in 1995. King (2010) reviewed in his thesis that a wiki consists of a collection of pages in which the user can open the wiki home page and create, edit or delete content using only a web browser. All

users have the same access rights to change a wiki's content. However, It can be argued that even a wiki has simple checking but has complicated security measures.

"The two key features of a wiki are its simplicity and flexibility" (Reinhold, 2006) cited in (King, 2010). A user need only have access to a web browser to use a wiki. There is no need for additional layout or links among the pages. "The expectation is that the internal structure will emerge from actual practice when using the wiki, and so be optimised to a user's needs" (King, 2010).

Figure 2.1: Screenshot of Wikipedia's site

Lindberg and Jensen (2012) defined the wiki as "an Open Collaborative Authoring System (OCAS) that relies on user contribution to generate the content it provides. They commented that the openness of wiki systems makes them ideal as knowledge sharing platforms to which everyone can easily contribute a small piece of the bigger picture. Moreover they pointed out that this feature may leads to be equally easy to delete good content or for malicious or incompetent people to add invalid information.

Wikis are described as one of the most popular web 2.0 technologies (Lv *et al*, 2010). It is also defined as "a collection of web pages designed to enable anyone who accesses it to contribute or modify content using a simplified markup language" (Foswiki, 2010).There are several types of Wikis depending on their usage, ownership and architecture. However, this technology is believed to have large possibilities for raising collaborative group work and creating learning resources.

In recent literature, Wiki is a foremost tool used for group assignments. Educational uses of wikis are popular topics in the recent literature. Nevertheless, several of these have addressed the problem of evaluating the contents that students have developed and the level of learning/competences reached in developing them. On the other hand, it would seem that evaluation of the collaborative process carried out by students has not yet been fully dealt with. (Strnad & Rugelj, 2010).

Strnad and Rugelj (2010) decided to use a wiki as a co-writing environment, to exploit its potential for:

- Redistributing responsibility for editing the overall document to all group members;
- Spurring on each participant, through specific group work organization, to collaborate in the various stages in producing the overall work; and establishing an evaluation mechanism based on analysis of the interactions among participants.

To fully benefit from the possibilities offered by wikis for co-writing and collaborative learning evaluation, the students' work should be organized so that everyone is motivated to play a part in each development stage of the shared script. "Co-writing

that is conducted online is almost always done so asynchronously and is mediated and indirect" (Weng and Gennary, 2004) cited in (Trentin, 2009). Therefore, students have greater opportunities to reflect deeply on what they read and write when replying to their remote interlocutors, besides practising their language skills. WikiSpaces was adopted for the experimentation, a choice made solely on the basis that this application is free of charge; it allows password access and both a classic and What You See Is What You Get (WYSIWYG) editor.

"Wikis enable information sharing and collaboration allowing learners to be actively involved in their own knowledge construction" (Trentin, 2009). Wikis have primarily been used in writing assignments, group projects and online/distance education although innovative uses in other areas can be found as well (Soon & Fraser, 2011). Trentin (2009) pinpointed some embedded wiki functions such as monitoring, tags, comments, linkers that support students' activities and their level of contribution to the collaborative work. Wikis allow students to meet virtually at their convenience and work on projects together (Soon & Fraser, 2011). Wiki can create a clearer picture of team direction than individual email messages as all interpretations and viewpoints are associated on one webpage

Leuf et al (2001) cited in (King, 2010) state that "wikis could support collaborative work in an educational background and enjoy the same advantages as wikis used in software engineering". (King, 2010) summarises the concept as being "the Wiki interactive pages model of collaboration allows participating members to actively work on the same materials online in order to be authors and readers at the same time, and to easily build information networks."

Wikis have simplicity and flexibility which makes them an engaging tool for content sharing and online collaboration. This has led to wikis being described as "the easiest and most effective Web-based collaboration tool in any instructional portfolio. Their inherent simplicity provides students with direct (and immediate) access to a site's content, which is crucial in group editing or other collaborative project activities" (Lamb, 2004) cited in (King, 2010).

Perez-Mateo and Guitert (2009) developed a virtual project in small groups to analyse how and why the students who start studying at the Universitat Oberta de Catalunya (UOC) use the wiki as a tool. The data analysis shows some conclusions in relation to the use of the wiki for the virtual construction of a project in small groups. They concluded that there are three main factors affecting the use of the wiki, namely, the degree of knowledge of the tool, the degree of difficulty in terms of usability, and the availability of time.

Researchers agree that social software like blogs, wikis, social bookmarks, podcasts, etc. increase collaboration, communication and knowledge production. Few studies analyse real practices that take place as a result of introducing these tools in a collaborative learning environment: how students use Web 2.0 tools, what are their motivations, etc. Such studies emphasize that changes by the introduction of social software go further than allowing the user to use tools from a technical point of view. The shift towards personalized learning environments implies the restructuring of educational processes.

Most of the literature emphasizes that wikis are a useful tool for sharing information among students and offers a place for students to get together essentially to discuss and personalize their learning experience. King (2010) commented in his PhD thesis that "the wiki can be successful in the learning use, but students need to be aware of good working practices because they will be writing the content in another tool, and then must

ensure the updated content is stored in the wiki for sharing with their peers."

Wikis foster learning through the exchange and sharing of information and opinions in a group. Goh Wei (2012) comments that wikis can deepen students' engagement in the learning process and encourage the co-construction of knowledge among peers. Furthermore, the use of wiki facilitates high-level thinking skills among students. (Lombard, 2007) cited in (Goh Wei, 2012) suggested that the effectiveness of wikis in facilitating critical thinking skills is dependent on the students' ability to validate and explain data and stand up to criticism. However, Anderson and Krathwohl (2001) cited in (Goh Wei, 2012) pointed out that "the majority of students engage in activities related to the application of knowledge rather than the evaluation of knowledge when they interacted with their peers in wiki." They suggested that learning activities need to enable serious decision and assessment criteria to involve the analysis and synthesis of information in order to participate students to think critically.

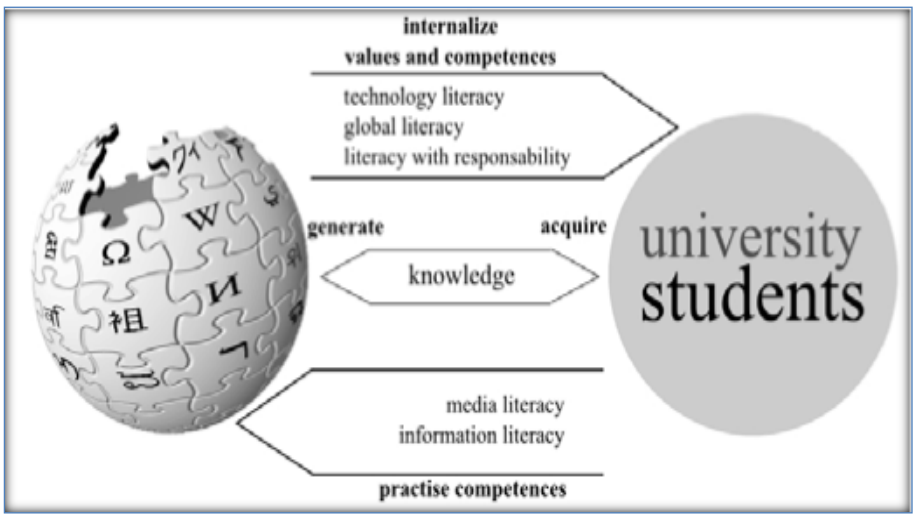


Figure 2.2: Flow transmission between the Wikipedia and University students by (Arribillaga, 2008)

Arribillaga (2008) claimed that "the Wikipedia allows universities to achieve the two

demands of our society nowadays: the generation of knowledge by students and the development of values and competences using wiki-technology-based systems" as shown in Figure 2.2.

Wikispace is a public wikipedia-based managed service which integrates the wiki with space, it illustrates the collaborative of wiki and the social of space, and it could be used to publish information, upload media and video. It facilitates the creation of pages easily, uploading of files and collaborative discussions. The current problems of special learning site can be solved, learners can create site models freely, create multi-mode in accordance with their own ideas. Because of its simple operation, low technical support, the learners develop website and build resources by themselves, it embodies the learner's autonomy fully (Jingbo & Yueliang, 2010).

B. Skype in learning

Skype is a communicating software application that allows users to make calls over the Internet to different parts of the world for free, while calls to both traditional landline telephones and mobile phones can be made for a nominal fee using a debit-based user account system.

The service allows users to communicate over the Internet with peers by voice using a microphone, video by using a webcam, and instant messaging. Phone calls may be placed to recipients on the traditional telephone networks. Skype has also become popular for its additional features, including file transfer, and video conferencing (Wikipedia, 2012).

Skype is used in educational settings mainly to add interactivity to the online courses. Students are able to chat with each other or the instructor over text/audio or video (Martin, 1996).

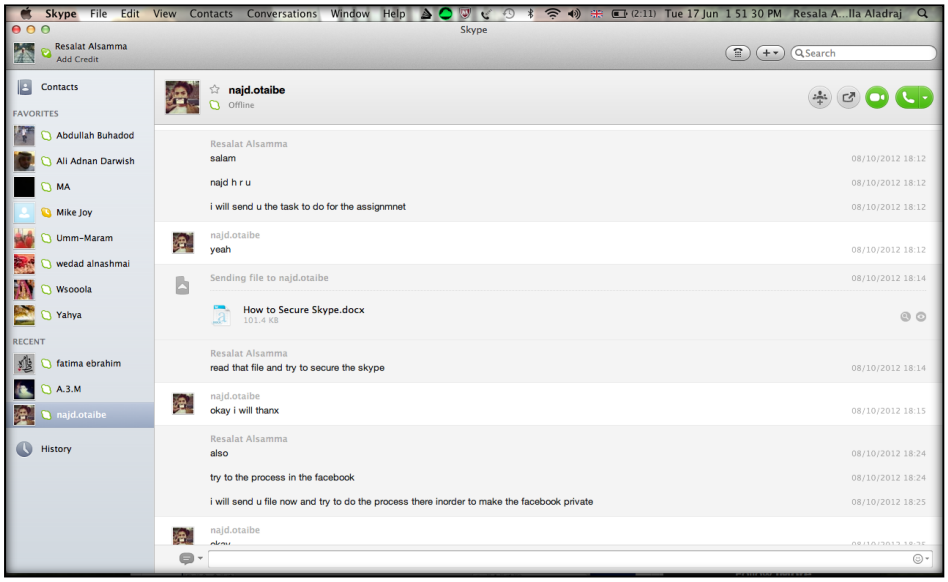


Figure 2.3: Screenshot of Skype chat during the Quasi-experiment

Skype is a simple and user-friendly multifunctional communication system that can be used for telephoning. The application provides a popular and straightforward way to keep in touch with friends, family and colleagues. Szedmina and Pinter (2010) pointed out that "the software is available in 27 languages and users implement it world-wide. While communication over the computer via Skype does not cost the user any money, there is a charge for calling landlines or cell phone numbers, using the voicemail and call forward options. The advantage of the application is that it is free, easily downloadable and its use does not require special IT knowledge. What it does require is a stable connection and a microphone, possibly a web camera for both the teacher and the students". These features contribute to the popularity of the Skype in learning. However, in the opinion of the authors, there are some of limitations such as:

Nevertheless, Skype is not a perfect tool for teaching large groups of students as the internet connection is unreliable used by the teachers and the students. and this may obstruct the teaching. Consequently, the web camera is unreliable .This would lead to a

stuttering web image which may have more of a negative than positive effect on the teaching process.

Martin and Noonan (2010) confirm the above advantages and disadvantages. They discussed in their paper the strengths and the limitations of the Skype as the following:

> "Skype is effective for instant messaging, audio/video chat, and file transfer applications as an increasingly popular and nearly ubiquitous solution. It is particularly effective for one to one student-instructor interactivity in the online environment. On the other hand, for video connections, the consumer grade versions of Skype only support point to point calls. In addition, the current version of Skype cannot support content sharing in native resolution; which can render some desktop content illegible."

Another advantage that can be considered is trustworthy. Skype has its reputation of a trusted tool and this will be discussed in Section 2.4.5.2.

C. Facebook as a teaching tool

According to (Zuckerberg, 2014) "Facebook is a well-known SNS with 1.28 billion monthly active users as of March 31, 2014. Moreover, a huge amount of information is shared on Facebook (1.317 billionposts every month according to (Smith, 2014)). Whereas Facebook has destructive effects, there has yet been little effort to investigate Facebook as an arena for collaborative learning. Judele *et al* (2014) claimed that "there is concern, however, about the quality of the information shared and about SNS's suitability for academic purposes, the use of tools and supportive learning systems for facilitating collaborative learning in computer environments is well established among educational scientists so far."

Facebook is being considered an educational tool because it enables peer feedback,

interaction, and learning in a social environment. Wei Wei *et al* (2013) confirmed that when they stated "The advances in Web 2.0 technologies have dramatically influenced learning and teaching. It has provided new learning opportunities and accessed to educational resources beyond those traditionally available such as Facebook". Facebook became very popular among University students for purposes of self-presentation. Facebook can facilitate collaborative learning as it can support the sharing of ideas.

Facebook's primary purpose was sharing information among friends and looking up people in our network. But it has explored possibilities of using Facebook as a teaching tool. Facebook has become a big part of students' lives and that is why Facebook could have great potential if used for education. "In 2006, 80 per cent of colleges in the USA had Facebook and in these colleges about 85 per cent of students had Facebook accounts" (Sheldon, 2008).

"In a survey where the main goal was to understand how contacts through Facebook were influencing student's perceptions of faculty, two thirds of the students reported that they are comfortable with faculty on Facebook site. They also found that "contact with the professor on Facebook had neither a significant positive nor negative affect on students' ratings" (Hewitt & Forte, 2006).

Facebook features can be used as course supplements. We can either use applications that are mostly developed by third parties and shared through Facebook or we can use features that are developed by Facebook. The latter group includes Facebook Chat, Pages and Groups. The researcher confirmed this by conducting the quasi-experiment which will be explained later in Chapter 3.

"We will first present Facebook applications and some examples of applications that can be used in courses and afterwards present other communicational and presentational features of Facebook which can be used in the educational process" (Nemec *et al*, 2011).

Leelathakul & Chaipah (2013) examined the effects of using Facebook to assist learning and teaching in classrooms on learners' performance. They found that "examining the proportion of number of Facebook posts and comments for educational purposes to the one for non-educational purposes could help us draw a conclusion that Facebook usage does have an impact on students' learning performances". Specifically, they found that students who spent more time on education-related posting and commenting gained better grades than the ones who did the opposite.

However, students may lack the encouragement and support from the lecturers, which leads to low level of adoption of Facebook as a learning tool. (Wei Wei *et al*, 2013) has conducted research in order to identify students' perceptions of using Facebook as a learning tool. This research demonstrates that there must be strategies to be followed by the lecturer as well as to set a clear plan for using Facebook. Wei Wei *et al* (2013) stated "The role and teaching strategies of lecturers need to be reconsidered. Lecturers need to set clear and relevant goals for the students when using Facebook as part of the teaching tool. Lecturers can motivate the student to construct their own knowledge and to be active in learning by participating in the Facebook discussion. Lecturers must not only adopt the role of participant observer but to create teaching presence to support the students all the time. As for the role of students, they need to be ready to utilize Facebook creatively for academic purposes".

Moreover, students may prefer to use Facebook to keep in touch with their friends and families for communicating rather than for learning. Wei Wei *et al* (2013), in the same research, studied whether Facebook is helpful, suitable and effective for academic purposes. The results showed that the majority of the students are indecisive about how helpful, suitable and effective Facebook is for their studies. However, the students preferred to keep in touch and communicate with their friends and family rather than

using Facebook for classroom-related activities (Wei Wei *et al*, 2013).

Facebook facilitates their interaction with others and improves content understanding in the class. Yu-ching (2011) conducted a study to investigate the differences of students' learning outcomes and satisfaction in a class using Facebook among different learning styles. Results showed that Facebook had a simple, convenient, easy, and user-friendly environment for academic discussions. Moreover, Yu-ching (2011) concluded that there is no difference in technology self-efficacy and atmosphere among different groups, since all four groups are moving towards high technology self-efficacy when using Facebook and agreed that Facebook provides a positive atmosphere for discussions.

Yu-ching (2011) had some suggestions in order to improve integrating Facebook in learning as follows:

- "Model messages need to be provided to decrease their anxiety to discuss in Facebook.
- There should be more editing tools in Facebook and enables users to organize their groups in Facebook. A reminder email is recommended to be delivered to participants whenever a new topic is created.
- Providing more course materials such as related readings, video clips, and power point files is also recommended to attract participants to learn in the Facebook environment.
- Entertaining films and messages may distract participants' attention from learning so appropriate configuration of online social networking tools is necessary" (Yu-ching, 2011).

D. Emails

In the late-1970s and 1980s, the phenomenal growth of personal computers (Apple II 1978 - 1985; IBM PC 1983 and Apple Macintosh 1984) created a whole new genre of

email technologies. Some of these systems were proprietary 'dial-up' systems such as MCI Mail, EasyLink, Telecom Gold, One-to-One, CompuServe, and AppleLink (Vicomsoft, 2014).

Some early email systems required that the author and the recipient both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Historically, the term electronic mail was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to describe fax document transmission (Wikipedia, 2014a).

Webmail is a web application accessed via a web browser. Emails are normally stored on the web-based email service provider's servers.

Popular examples of web-based email services include Gmail, Hotmail and Yahoo Mail. "Practically every webmail provider offers email access using a webmail client, and many of them also offer email access by a desktop email client using standard email protocols, while many internet service providers provide a webmail client as part of the email service included in their internet service package"(Wikipedia, 2014b). Webmail provides the ability to send and receive email anywhere from a web browser. This feature makes it useful.

E. Email usage

"The Technology Acceptance Model (TAM) predicts whether users will ultimately use software applications based upon causal relationships among belief and attitudinal constructs that influence usage behaviour. Electronic mail, or email, is a collaborative technology available to virtually all members of an organization, and typically, there are alternative email applications available for use" (Hubona & Burton-Jones, 2003).

Hubona and Burton-Jones (2003) applied TAM to assess the user acceptance and voluntary usage of a particular email application, cc:mail, in two different organizations. "The results largely validated TAM, although the findings suggested that certain external variables – namely length of time since first use, and level of education – directly affect email usage behaviour apart from their influence as mediated through the perceived usefulness (PU) and perceived ease of use (PEOU) constructs."

F. Emails in learning

Technology can offer the means for students with to communicate via email and use the internet for research, and can also help teachers familiarize students' varying learning style. Skilled students can explore subjects in more complexity than the basic syllabus and they can work with their own limits. "The powerful tools of technology allow every student access to the vast resource of information about the world" (Ning & Bao, 2010).

Email allows students to collaborate with people not physically present over large distances. Indeed, Email can motivate the students to improve their reading and writing skills.

Thao and Quynh (2002) pinpointed that "communication has been widely used in tertiary education. It should be used to enhance teaching and learning." They conducted a study over two years with university students in an academic program in order to explore the utility of email communication from the learner's perspectives. A total of 1478 students' emails were collected for data analysis. They found that "students' email communication was heavily based on management of learning. They were more concerned with clarifying, confirming, requesting to ensure that they were on the 'right track' and little emphasis was placed on discussion of ideas and concepts." (Thao & Quynh, 2002).

2.3.5.4 Conclusion

The literature and examples of the use of OCG tools suggest OCG must provide some communication tools such as e-mail, Wiki, blog, chat, and video conference that fulfil the requirements of collaborative learning to exchange information, coordinate actions and to reach agreements

This conclusion, together with this from 2.3.5.3 needs to be examined more closely to see if this is also true where social context has an important role in interpersonal communications, which directly determines if the two parties can communicate and collaborate with honesty, trust, and openness.

Generally speaking, the teaching methods used are still very traditional. The use of communication tools such as email, Wiki, and Facebook should improve the pedagogical process by improving students' involvement and motivation in learning but their use depends on the willingness of educators to use different methods of learning, teaching and assessment. We concluded that Facebook is the most popular tool for communication/chat and such Facebook features can be used as course supplements. However, email allows students to collaborate with each other whilst not physically present, over large distances, and this affects their engagement.

2.4 Security, Privacy, and Trust

The Privacy, Security & Trust mechanism is about understanding how information technologies impact the privacy of individuals and developing new secure technologies to protect them. For the purpose of the research, the following are the terms which give some information about these mechanisms.

2.4.1 Security Technologies

Security means that information shared by the tool will only be accessible to those for

whom it is intended, while privacy means the ability of an individual or group to isolate information about themselves, and thereby reveal themselves selectively.

Security and privacy are closely related technologies, however, there are important differences. Privacy is about informational self-determination – the ability to decide what information about you goes where. Security offers the ability to be confident that those decisions are respected (Bergeron, 2000).

Moreover Chade (2011) clarify the differences between secrecy and privacy as "The essential difference between secrecy and privacy as security concepts that secrecy attempts to hide information that can be gleaned through simple observation and analysis from others, while privacy attempts to keep communications between people from being intercepted. The two are easily conflated at times because the security technologies of privacy – including access control, encryption, and verification – are the very technologies employed in the pursuit of secrecy. Because of the fundamental inefficiencies of secrecy, however, such technologies are constantly subject to failure, and that failure often has nothing to do with the technologies used."

2.4.2 Trust

Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another (Rousseau et al, 1998). Pearson & Yee (2012) discuss in their paper that trust is a broader concept than security as it includes subjective criteria and experience. Also he pointed out "there exist both hard (security-oriented) and soft trust (i.e. non-security oriented trust) solutions. "Hard" trust involves aspects like authenticity, encryption, and security in transactions, whereas "soft" trust involves human psychology, brand loyalty, and user-friendliness. Some soft issues are involved in security, nevertheless. An example of soft trust is

reputation, which is a component of online trust that is perhaps a company's most valuable asset." Soft trust will be considered in this thesis.

2.4.3 Technology Trust

Technological solutions are not only designed to keep users safe from any threats, but also to increase ''trust''. According to May and George (2011) trust is defined as a confidence in someone's competence and his or her obligation to a goal. Trust is also vital to enable meaningful and commonly beneficial interactions that construct and maintain learner collaboration and community. At the moment, privacy and trust are fundamentally connected as privacy is a natural concern, increasing the importance of trust in any learning environment. For example, in a closed learning environment – where all learning services are provided internally – students can have higher confidence that their personal data will be treated properly. Thus, working collaboratively with other learners could be effectively conducted upon trust.

Pentafronimos *et al* (2011) stated "both collaborative workspaces and social networks have efficient features such as user-generated content and potential disclosure of Personally Identifiable Information (PII) during the process, while both are generally susceptible to the same security threats caused by the integrated web 2.0 technologies". On the other hand, they believed that the dynamics of privacy are different for social networks, as "users must specifically agree to reveal their PII in order to participate in the network and gain benefit from the offered services."

They also stated new measures and protocols are needed to assure trust and protect user's privacy such as:

- “Privacy should be protected against users’ capability to post violating content and other privacy pervasive information;
- Reporting of inappropriate behaviour and posting of privacy pervasive information is considered essential;
- Access control and privileges allocation should be based on users’ behaviour, leading to trust or distrust that emerges as a result of opinions of members of a certain community.”

Thus, in order to evaluate the possible risk dynamically and asynchronously, the shared knowledge about user’s trustworthiness must be provided as the input to authorization decisions.

2.4.4 Authentication

The process of confirming the personal identity is called authentication. It involves checking the identity of a person by confirming their identity documents and validating the legitimacy of a website with a digital certificate.

“authentication is also defined as “ the process of determining whether someone or something is, in fact, who or what it is declared to be” (Rouse, 2014a).

One of the authentication methods is the use of logon passwords in the Internet as the password is supposed to assure that the user is authentic, and this is commonly used. However, this technique has weaknesses in that passwords can often be stolen, accidentally revealed or forgotten.

2.4.4.1 Signing and encryption

(Rouse, 2014b) stated that a “digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and

possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real".

2.4.4.2 Security's attack methods and solution

Adeyinka (2008) stated some common Internet attack methods and some different internet security technologies. Adeyinka (2008) showed the relationship between the various attack methods and their corresponding Internet solutions in a table below.

Table 2.1: Attack methods and solution

Computer security attributes	Attack methods	Technology solutions for Internet security
Confidentiality	Eavesdropping, hacking, phishing, DOS, and IP spoofing	IDS, Firewall, Cryptography systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DOS and IP spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, spamming, hacking, DOS and cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DOS, email bombing, spamming and systems boot, record infectors	IDS, Firewall, Anti-Malware Software and Firewall

Security plays a significant role in the development of groupware systems. Standard security provides the groupware with the integrity, confidentiality, and the availability to protect the collaborative groupware from threats. A critical element of groupware security is groupware access control.

With the development of original enabling technologies such as peer-to-peer systems and web services, different types of collaboration systems are developing. For example, user interaction and access to information and services are increasingly performed across organizational boundaries. Generally, the internet has introduced new security threats such as denial of services, which is an effort to make a machine or network resource inaccessible to its intended users.

A trust approach is needed for accessible and adaptable access control in online collaborative groupware. The following will look at trust and technological solutions.

2.4.5 Role of security in the collaborative e-learning environment

Recently, in the collaborative e-learning environment users need to reveal their private information and identities because they need to create user profiles which could disclose more information about the user than he wants to give. Thus conserving privacy is an essential factor of such environment. Therefore, security in e-learning is needed as Bourimi *et al* (2009) claimed "The role of security in e-learning is to protect authors' e-learning content from copyright infringements, to protect teachers from students who may undermine their evaluation system by cheating".

In order to address the role of security in the collaborative e-learning environment, Raitman *et al* (2005) conducted a case study to test the sense of security that students experienced whilst using the wiki platform as a means of online collaboration in the

tertiary education environment. They set up two units with similar principles in a wiki environment, with the only difference being that one had a user login requirement. In the other unit, users had complete control over their actions, with no accountability, nor the fear of being accused of misconduct. As a result of their case study, they perceived "the value and benefits of fostering a sense of security in the online e-learning environment."

2.4.5.1 Facebook and Privacy

Since Facebook Chat was introduced in 2008 it still has a large user base. However, Facebook is not secure, as it does not transmit data over HyperText Transfer Protocol (HTTPS) by default. This means spies on the network have possible access to Facebook Chat conversations. Robison *et al* (2012) pointed out that "Facebook users need to explicitly turn on HTTPS in Facebook's account settings for the browser to communicate with Facebook over an encrypted channel. Even if a user secures their own connection to Facebook, there is no way to guarantee that the other party in a chat session also has HTTPS turned on."

This comment in my opinion is not correct all the time. HTTPS is not always secure and can be spoofed by third parties in middle of client and websites.

2.4.5.2 Privacy and Skype

Skype is extremely widespread for making calls and sending instant messages. Part of its fascination is because it's cheap and easy to use. However, many people such as journalists and dissidents also use Skype because they believe it is safe from surveillance and eavesdropping. Ever since it was founded in 2003, Skype has been favoured by journalists and human rights activists around the world because of its reputation for privacy and security. However, there are some things journalists should be clear on when using Skype (Hairsine & Karbasova, 2013).

When Skype is used to communicate with clients and business associates, the security of the network is highly important. “Confidential matters that are discussed in text chat, voice chat or video chat – as well as files sent from one person to another – are protected by several different layers of security” (Parker & Media, 2014).

Skype uses multiple kinds of privacy, user authentication and data encryption (such as verification codes). Also Skype issued a digital certificate which identifies the user as the owner of the Skype account – every other Skype user has their own digital certificate as well.

For the purpose of the research and to simplify the experiment for the students, privacy settings of Skype were chosen as seen in appendix C for protecting their privacy. This mechanism allows them to decide who can directly call or converse with them. However, even if privacy settings are set, there is still a chance of receiving “Hello from” requests from new visitors.

2.4.5.3 Security and Wikis

The ability of anyone to edit the content is, at the same time, a wiki’s strength and weakness. Anyone can write documents that improve the value of the wiki-system, but at the same time, anyone can also introduce errors into these documents, by accident or on purpose.

Wikipedia has set some of rules to protect the wiki user account. “All registered users have to log in using a password before they can edit using their usernames. Passwords help ensure that someone does not masquerade as another editor. Editors should use a strong password to avoid being blocked for bad edits by someone who guesses or "cracks" other editors' passwords…. on Wikipedia, only certain users

(including administrators) can perform some actions. It is especially important that these privileged editors have strong passwords" (Wikipedia, 2014C).

"Wikipedia is the largest encyclopaedia on the Web which is based on crowdsourcing, the process of outsourcing a task to a large group of people, in the form of an open call. The crowdsourcing approach stands in sharp contrast to more traditional models of content creation and publication, which tend to limit content creation to a relatively small group of approved editors in order to exercise strong quality control. Because of its open editing model -allowing anyone to enter and edit content – Wikipedia's overall quality has often been questioned" (Javanmardi *et al*, 2009).

Javanmardi *et al* (2009) conducted a study to provide an analysis of the open editing model of Wikipedia. The study's objective was to compare the behaviour of anonymous and registered users from different aspects. The results show that the following:

- "the majority of the revisions are submitted by a small percentage of users, and that most of them are registered users."
- "the results show that there is a positive correlation between user registration and the quality of contributed content."
- "the distribution of user reputation in Wikipedia also shows that, regardless of attribution, vandals and inexpert users are still quite a minority compared to high reputation users."

Thus, Javanmardi *et al* (2009) recapped that "it appears that the open editing model of Wikipedia relies on a large number of well-intentioned users who actively contribute in such a way as to neutralize any vandalism or poor quality content that may be inserted by the smaller number of problematic users."

According to Wikispaces, there is a permission that allows the user to define who can

See, edit, and interact with their wiki or label the site as private.

"Every Wikispaces wiki will let the user set permissions at both the wiki and the page level, so access can be more restrictive at every level. For example, a wiki can be set to public, but a single page can be locked – so anyone can see or edit most of the wiki, but only organizers can edit that one page" (Pentafronimos *et al*, 2011).

2.4.5.4 Emails Security concepts

Despite the age of email, concepts have changed little. "Certainly, developments have taken place; but the main protocols remain the same. In email concepts, it exists two main classes of protocols; message format and its routing" (Cailleux *et al*, 2014).

The first emails did not have any security services and the policies were limited. With the threats evolving, new security objectives and security properties have been identified. The following are the security properties of the security services which have been defined by Cailleux *et al* (2014):

- Non-repudiation of origin
- Data integrity
- Data origin authentication
- Data confidentially
- Authorization

They cited in their paper that "in order to apply these properties, two mechanisms have been stated: cryptography signature and encryption services"

Cailleux *et al* (2014) stated that Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension S/MIME) are the protocols which provide email signature and email encryption services. "S/MIME is based on a centralized trust model and needs a

Public Key Infrastructure (PKI), a trusted third party to provide authenticity of public keys. PGP is based on a decentralized trust model also called Web of Trust. They are oriented towards end-to-end communication and most email clients are compliant with these standards."

2.4.5.5 Secure emails

Spam and Phishing

Spam has great impact on the emails. It challenges the safety and usefulness of email. In addition to that it is time and cost consuming. (Solic *et al*, 2011) defined spam as "unwanted and unsolicited email, that has usually been sent to many recipients."

Spam is considered the major source for flooding network traffic as (Ghafoor *et al*, 2009) commented . They stated that spam creators abuse authorization weaknesses of the original email standard in which anybody can send email to any other user.

Spam can contain attachments that contain text, images or URLs and these are responsible for phishing attacks. Also, spam can contain executable files, such as viruses, worms or Trojans.

Email usage has been increasing along with the growth of unwanted side effects: viruses, worms and spam. Indeed, spam and fraudulent email messages are major concerns for email users. "Spam was once just an annoyance, but it has now become the tactic of choice for online deception, fraud, and abuse. the freedom of communication is being , issued and has become a threat to email communication society" (S.Dhanaraj & V.Karthikeyani, 2013)

According to (Dhanaraj & Karthikeyani, 2013) reported that "spam emails have been grown by more than 10 percent during 2009 and spam proportion of total email volume is more than 92 percent during the same year …this statistics is expected to grow in

forthcoming years, which stresses the fact that threats to email communication are increasing at a massive and unchecked pace".

Recently, numerous filters were developed to detect or prevent text-based spam mails. However, some spammers put their spam contents into image in order to bypass text based anti-spam filters.

There are a lot of spam categories, namely, products advertisement, financial, adult, internet, health, etc. but the email attacks that appear to be from a well-known organization are called "phishing". Phishing is one of the methods that fool people into revealing their personal information by using social engineering and technical tools without using any of the common fraud methods such as sniffing, Trojan horses or viruses.

Salem *et al* (2010) point out that "Anti-phishing group (APWG) defined phishing as "an attack that uses both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials."

Phishing is one of the most effective online scams and is categorized as a criminal action. This action costs businesses thousands to millions of dollars yearly and personal client data can be lost.

Salem *et al* (2010) has listed different kinds of phishing techniques such as impersonate, forward attack, pop-up attack, voice phishing, and mobile phishing.

Several techniques have been proposed to reduce the risk of phishing attacks.

Salem *et al* (2010) listed some of them, namely, anti-phishing toolbars, browser plug-ins, and email-filters.

These techniques are not sufficient to protect the emails from such kinds of attack, human awareness and education are needed. These techniques are most successful to protect the users from the malicious attacks. Security education, training and awareness

programs have proved to be the most successful regarding protecting end users against malicious attacks" (Mann et al 2008) cited in (Jansson & von Solms, 2011). However, many of the end users do not pay attention to such awareness techniques. (Jansson & von Solms, 2011) mentioned the reasons for this is that:

"One reason for this may be that the users believe that they are already familiar with the material. On the other hand, many users are actually less vulnerable since they are aware of such attacks. Therefore, spending resources on training these 'aware' users would be pointless. Likewise, if all the users, including 'aware users' spend several minutes a day learning how to protect themselves, the cost in terms of 'user time' would often be greater than the resultant cost of such an attack"(S. Furnell,2005) cited in (Jansson & von Solms, 2011).

2.4.5.6 Trusted emails

Almadhoun *et al* (2011) have conducted a study in order to identify the effect of security, privacy, and trust in Social Network Sites (SNSs), for the purpose of sharing information and developing new relationships in order to discover how it affects students' enrolment. In doing this, they conducted a survey of 66 participants. Their findings suggested "that perceived privacy and perceived trust in other members in SNSs is significantly related with the Information sharing. Also, members' trust in SNSs and its members positively associated with development of new relationships, which is positively associated with students' enrollment and employees' application in HEIs. However, there is no significant impact from information sharing to develop new relationships in SNSs." (Almadhoun *et al*, 2011).

Brush & Borning (2005) researched 'today' messages, which they defined as "short status emails sent daily by members of a project team". They identified privacy,

accountability, and trust as “the values most strongly implicated by ‘today’ messages, based on our initial analysis and own experience with their use. While ‘today’ message are self-reports, they still ask individuals to report on their activities, possibly raising privacy concerns. Their frequency also means individuals are reporting their accomplishments on a daily basis both to their groups and managers, significantly changing the granularity of accountability in comparison with the more common weekly, monthly, or quarterly reporting. Our early investigations also suggested that trust among group members would be important for the success of ‘today’ messages.

There are some techniques used to counteract phishing attacks. Crain *et al* (2010) have indicated two of them: “Browser toolbars and email verification”. Microsoft Internet Explorer and Mozilla Firefox are the most popular web browsers that include anti-phishing features. For example eBay have a tool that can identify eBay pages (eBay, 2007b). Additionally, Google have a tool that aim to identify fraudulent websites (Google, 2007a). However, most studies has shown that these tools are ineffective in recognizing phishing.

2.4.5.7 Fighting Phishing with Trusted Email

“Phishing is a combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker (phisher)” (Crain *et al*, 2010). Reading email has become an unsafe activity. Emails can carry dangerous viruses and worms that can be executed by the ordinary act of opening the email, opening an attachment, or clicking on a picture. Phishing attacks are increasingly common, and typically use spoofed emails that trick users into revealing their private information. Phishing emails are usually hard to distinguish from legitimate emails and phishing web sites look just like legitimate web sites.

The most important feature of a secure email system is usability. In practice, users will rather use an insecure email system that is easy to use than a secure email system where even the help text seems intimidating. The secure email system has to be easy enough to use when compared with simple, familiar, regular email systems − not when compared with other secure email systems. If security is too difficult or annoying, users may give up on it altogether (Gerck, 2007).

In summary, to support usability, the technology should have simple, effective rules allowing complex patterns to be expressed as desired, rather than rules that require complexity from the start. Usability can be technologically provided by the presence of usability features as well as by rejection of usability problems, with reduction and simplification of all rules.

2.4.6 Security Culture

"Security system, however sophisticated the screening technology, can be significantly influenced by the attitudes and behaviour of personnel and the supporting security policies … Culture is of interest in a security context if it can be proven to affect security outcomes" (Malcolmson, 2009). Therefore, understanding and then enhancing the security culture among the students where security is a critical success factor is likely to lead to those students being better able to use OCG tools.

Siu Man and Hui (2011) conducted an experiment in order to find the effects of information security knowledge on user's adoption of security technologies. They concluded from their experiment that "security technology adoption involves decision-making under risk and uncertainty". They manifested that knowledge can be used to minimize risk and uncertainty associated with security decisions. Thus, it is important to understand how knowledge affects security decisions, "especially when education,

training and awareness programs are one of the most suggested strategies to change human security behaviour".

2.4.7 Conclusion

This section defined the security technologies, privacy and trust and their role in collaborative environments. It was shown how Facebook and Skype privacy can serve the teaching. Moreover, we recapped that wikis has a malicious user minority compared to high reputation users. The subsequent sections critically reviewed literature on the aspects of security and the emails relevant to this research, to define the main research questions that will be shown below.

The special interest of this study was how to deploy the aspect of security in emails, and how the study of security and trust can enhance the usage of emails in the learning process among collaborative students.

2.6 Chapter summary

The literature review clarified that the students' learning styles and their ability to use technology must be taken into consideration both inside and outside the classroom. Students' trust in the OCG tools affects their motivation and learning which can lead them to awareness of security technologies. The researcher began with describing the technological aspects that support the learning which has been clarified in the first section of this Chapter. The research presented in this Chapter is summarised as follows:

- How wikis can be used as co-writing environment;
- How Skype is able to be utilized as a chat tool with the students talking to either each other or an instructor. Skype is being used in the educational setting mainly to add interactivity to the online courses. Students are able to chat with each other or the instructor over text/audio or video (Martin, 1996);

- Email is a tool that can allow every student access to the vast resource of information about the world (Ning & Bao, 2010);
- Electronic mail, or email, is a collaborative technology available to virtually all members of an organization, and typically, there are alternative email applications available for use (Hubona & Burton-Jones, 2003);
- Hubona & Burton-Jones(2003) applied the Technology Acceptance Model (TAM) to assess the user acceptance and voluntary usage of a particular email application, cc:mail, in two different organizations. The (TAM) was discussed as it is used as a basic for the research framework.
- How authentication technologies such as signing and encryption and anti-phishing and spam tools should be used to allow emails to be trusted by the users.

These statements are used as the basis of the hypotheses for the present research and will be tested in a course of study with the students. The initial hypotheses for the study will be discussed in Chapter 3. In addition to that, a detailed initial study will be conducted and discussed to further analyse the need for secure and trusted emails in the learning. For this, improvements on the TAM model have been proposed and amended them to be more suitable for the students undergoing the research experiments and activities.

Chapter Three: Research methodology

3.1 Introduction

This Chapter will provide an overview of the overall process and different stages of the research, the principles upon which the study is based and the different research techniques that have been chosen to gather sufficient and relevant information in order to fulfill the objectives of this study.

In this Chapter the mixed methods approach has been introduced to investigate the usage of secure collaborative groupware tools by a group of undergraduate students in Bahrain.

The methodology has been carefully developed keeping in mind the purpose of the exercise and the research questions to be answered. The identified research objectives have been the guiding factor in determining the appropriate research methodology in this study.

3.2 Research Objectives

Determining the purpose of any research task is of utmost importance as, without preset objectives, decision-making is uncoordinated. When undertaking a project, the purpose and boundaries must be defined in order to avoid project creep.

As a guide, the entire research strategy is divided into five stages, as described in Table 3.1 below. Each stage has its own objective, which are summarized below for the benefit of the reader.

Table 3.1: Determining Objectives of the study

Chapter Number	Stage/Activity	Research Objectives
Chapter 4	**1A**.Student Survey	To determine the difficulties and problems faced by Bahraini students when they use OCG tools.
Chapter 4	**1B.**Interview	To determine the difficulties and problems faced by Bahraini students when they use OCG tools.
Chapter 5	**2.** Quasi-experiment	To figure out the perception of the students of the security, safety, and privacy when using OCG tools during the learning activities
Chapter 6	**3.** Secure email awareness's evaluation	To reveal the students 'awareness of secure email.
Chapter 7	**4.**Email tracking intervention	To find out a clear picture of secure email usage and awareness.
Chapter 8	**5.A.** Case study	To investigate solutions for improving the usage of email in the learning by the undergraduate students at the University of Bahrain
Chapter 8	**5.B** Evaluation	To determine the effectiveness of the security and trust on the actual usage of the email in the learning.

3.3 Definition of Methodology

Methodology is defined as:

(1) "a body of methods, rules, and postulates employed by a discipline",

(2) "a particular procedure or set of procedures", or

(3) "the analysis of the principles or procedures of inquiry in a particular field" (Nance, 1994, p. 2).

Research methodology refers to more than a simple set of research methods; rather it refers to the overall rationale and the logical assumptions that underline a particular study.

3.4 Research Methodology

An overview of all the stages is provided in this section of the study and shown in Table 3.1. All these procedures have been carried out and the stated methodologies adapted as the basis for addressing the research objectives and questions. Therefore, the methodology detailed above acts as the basis for this study and provides the framework needed for data collection and data analysis.

3.5 Research Method

The researcher adopted a mixed method approach in this study. Both qualitative and quantitative data were collected from students and analyzed extensively in this study.

3.5.1 Qualitative data

The qualitative data of this study includes non-numerical data obtained from interviews conducted with some of the participants and their teachers, and its interpretation.

In this study, the researcher used qualitative data at stages 1 and 2 to conduct interviews with UOB students. In addition, the researcher resorted to qualitative method at stage 5 in order to conduct observations, as highlighted in Table 3-2.

3.5.2 Quantitative data

Quantitative data communicate meaning and interpret information by means of numerical analysis. This is accomplished by statistical methods that help to generalize findings. Quantitative researchers take an objective stance regarding participants and their settings, and use sample research to apply their findings to a larger population

(Neuman, 2000; Dillman, 2000).

The quantitative data of this study emerges from the 5-point Likert Scale questionnaire used in this study, and its analyses.

3.5.3 Mixed method

Using more than one research method for data collection to achieve the research aims and objectives is known as a Mixed Method. The mixed method of data collection used in this study employs both qualitative and quantitative methods as they are regarded as highly complementing rather than mutually exclusive to one another (Creswell, 2003). Moreover, the mixed method of data collection allows the researcher to do "triangulation", which was first developed by Campbell and Fiske (1959). However their work did not use the term "triangulation". This Seems to have been applied to their approach later by Webb et. al.(1966).

3.5.4 Triangulation

Leedy (1997) defined triangulation as the way in which different methods of data collection, varying data sources, different analyses or theories can be used to check the accuracy and validity of the findings. Creswell & Miller (2000) puts forward the argument that the use of varying methods of data collection and analysis should lead to greater validity and reliability than a single method of data collection and analysis. Therefore, both qualitative and quantitative methods were used for the purpose of triangulation. The researcher is of the opinion that by deploying the qualitative and quantitative method data collection and analysis, the credibility of findings and interpretation of the findings can be enhanced as the evidence and theme emerges from different sources.

3.6 Research Design and Approach

Various methodologies are implemented in research, each serving a different purpose and providing a different outcome. Researchers need to understand what information they wish to obtain prior to the collection of data. Babbie (1990) indicated that research methods include analysis of existing data, case study, controlled experiment, interview, questionnaire and participant observation.

Table 3.2: Chosen Method for each stage

Activity/stage	Data collection	Method	Aim
1A. Pre-experiment Student Survey	Questionnaire	Quantitative	To find the students' perception of the tested OCG tools.
1B.Pre-experiment Teachers/Students Interview	Interview	Qualitative	To establish if there is common feedback among teachers. And to find the students' feedback
2. Critical case study 2.1 Keeping track of every action occurred with SWFG	Log files	Qualitative	To gain a sense of how participants navigate through SWFG.
2.2 Post-experiment Student Feedback	Questionnaire Observation	Quantitative Qualitative	To evaluate the security, safety, privacy and trust of SWFG tools. To discover if there is a common behavior for students during the experiment.
3.Secure email awareness evaluation	Questionnaire	Quantitative	
4.Secure email	Emails tracking form	Quantitative	
5.Quasi-experiment	1.interviews 2.questionnaire	Qualitative Quantitative	

In the present study, different types of data collection methods were used at the different stages of the research. The details of the data collection methods and the reason for choosing these methods are summarized in Table 3.2 above.

3.7 Questionnaire Survey

The researcher planned to conduct some questionnaire surveys at varying stages of the study. Those questionnaire surveys carried out with the students were conducted through a questionnaire distributed to the students in the classes.

According to Milne (1999) from the Centre for CBL in Land Use and Environmental Sciences, Aberdeen University, there are certain advantages and disadvantages of conducting such a questionnaire, as discussed below.

3.7.1 Advantages

- The responses are gathered in a standardized way, meaning that questionnaires are more objective, certainly more so than interviews.

- Generally speaking, it is relatively quick to collect information using a questionnaire. However, in some situations they can take a long time not only to design but also to apply and analyze

- Potentially information can be collected from a large portion of a group, although this potential is not often realized, as returns from questionnaires are usually low. However, return rates can be dramatically improved if the questionnaire is delivered and responded to in class time (Institute for Computer Based Learning, 1998, p.52).

3.7.2 Disadvantages

- As many evaluation methods occur after the event, participants may forget important issues.

- Questionnaires are standardized so it is not possible to explain any points in the questions that participants might misinterpret. This could be partially solved by piloting the questions on a small group of students or at least friends and colleagues, which is advisable in any case.

- Open-ended questions can generate large amounts of data that take a long time to process and analyze. One way of limiting this would be to limit the space available to students on the questionnaire itself so that their responses are concise, or to sample the students and survey only a portion of them.

- Respondents may answer superficially especially if the questionnaire takes a long time to complete. The common mistake of asking too many questions should be avoided.

- Students may not be willing to answer the questions, as they might not wish to reveal the information; or they might think that they will not benefit from responding, perhaps even being penalized by giving their real opinion. Students should be told why the information is being collected and how the results will be beneficial. They should be asked to reply honestly and told that if their response is negative this is just as useful as a more positive opinion. If possible the questionnaire should be anonymous (Institute for Computer Based Learning, 1998, p.52).

3.8 Details of participants, number and selection method

The researcher chose the students of UOB and Arab Open University in order to conduct each stage. Participants' details will be explained in each Chapter according to each methodology.

3.9 Chapter Summary

This Chapter outlined the entire research methodology used in this study. The actual detailed methodology will be discussed at the relevant stages of the research activities in the following Chapters.

In the next Chapter, the researcher introduces the case study which was figure out the perception of the experimental group (B) of the security, safety, and privacy when using OCG tools during the learning activities, with a particular focus on the impact of their usage on the trust and motivation of the students. Skype, Facebook, Wikis and Gmail (SWFG) were the OCG tools used in order to apply the case study. Details of these are presented in Chapter 4.

Chapter Four: Initial study

4.1. Introduction

This Chapter introduces the primary research conducted in this study to identify the fundamental issues and problems faced by both students and teachers while applying OCG tools such as Instant Messaging, Skype, Webmail, Facebook, etc., as discussed in Chapter 2 of this study.

This primary research is necessitated by the fact that the researcher needs to identify the problems currently faced by students and teachers when learning using OCG tools to confirm the problem statement presented in the introduction to this study. The primary research was conducted among students and teachers in UOB with the wider objective of monitoring the experience of OCG tools usage in Bahrain.

After collecting the initial data from the primary research, the researcher proceeded to concentrate on Skype, Wikis, Facebook, and Gmail (SWFG) only. This was due to the feasibility and ease of working with such tools as most of the students and the author are already familiar with them.

4.2 Student Questionnaire Survey

4.2.1 Introduction

In the light of the literature review, the lack of students' trust, and, consequently, their lack of motivation, has been investigated as a major problem which relates to the OCG tools. Another issue identified is the lack of awareness of how to use secure OCG tools.

In light of the above, a questionnaire was used to verify these problems with UOB students and teachers. Additionally this allowed for the identification of appropriate

activities to validate the research framework allowing the research to focus on solving these issues.

4.2.2 Aims of the student survey

Surveys are defined as "useful methods to gain an overview of a particular situation, which are often used by policy makers and by those who wish to inform policy makers." (Birley and Moreland,1998).

The questionnaire-1 (online and paper-based exploratory questionnaires) was found to be the most suitable method to collect the required feedback, opinion and experience from users of collaborative tools in order to identify what kinds of security problems they face (See Appendix A). The descriptive method was chosen because it suits the aims of this Chapter to collect views about the experience of students when learning using OCG tools.

4.3 Methodology

This section will describe research methods along with the principles upon which the study is based and the different research techniques that have been chosen to gather sufficient and relevant data in order to fulfil the objectives of this study.

4.3.1 Quantitative research methods

4.3.1.1 Validation

The questionnaire was initially sent to 10 PhD candidates in the Computer Science department at Warwick University to test the readability of the questions. Moreover, the contents validation was applied in order to confirm if the contents suits the objectives of this Chapter. Contents validation is defined as "The extent to which the items of a test or procedure are in fact a representative sample of that which is to be measured; e.g., items relating to ability in arithmetic and defining words are appropriate content for an

intelligence test." (Mondofacto, 2000)

After validation some minor modifications and alterations in the writing style and contents related to security were made. Then, the reliability of the questions which use Likert–like scales has been check using SPSS, and the result was 0.77. Data from pilot respondents were not used in the main study.

4.3.1.2 Respondents

. The paper based and online questionnaires were distributed among 200 undergraduate students in UOB. 187 respondents answered the questionnaires. The collected data was analysed using SPSS software to address the main research questions of the study.

4.3.1.3 Questionnaire design

The first section of the questionnaire-1 (See Appendix A) was designed to understand the demographic background of the students, covering gender, age, course studied and experience in using LMSs.

The second section focused on obtaining information about the respondents' experience of some of the most familiar OCG tools in the web as discussed above. In addition, the researcher desired to obtain the participants' feedback about most desirable features of OCG tools that provide them benefit.

The third section of the questionnaire covered general questions regarding the respondents' awareness of security technologies such as authentication and authorization.

The fourth section asked the respondents questions about the type of assessment they prefer and which types of information they think their teachers provide in order to deliver a course efficiently using OCG tools.

4.3.1.4 The scale used in the questionnaire survey

Likert scales 1-5 were used in Section 2 (question 6) to acquire quantitative data and therefore facilitate data analysis of this study. The scale is from 5 (Very effective) to 1 (Completely ineffective). In the scale of 1-5, the median is 3 (defined as neither effective nor ineffective) for the purpose of this study as shown in Table 4.1.

Table 4.1: Likert scales used for question 6

Scale used in the questionnaire	Description
5	Very effective
4	Effective
3	Neither effective nor ineffective
2	ineffective
1	Completely ineffective
0	I have not used this tool

4.3.1.5 Analysis of student questionnaire results

A. Students' perception of the efficiency of the OCG tools

Figure 4.1 illustrates the opinion of the respondents regarding the usage of CSCL tools. There are 10 tools in total, including Instant Messaging (IM), social media, forums and email.

A sample of 200 respondents was taken for the survey, each of whom was asked to judge the effectiveness of the tools.

Out of 187 respondents, the majority (72%) regarded IM, social media and forums as effective, while 49% of the respondents chose IM, social media, document sharing and telephones as very effective. Email was also chosen as a very effective tool by a significant proportion of those surveyed (80%).

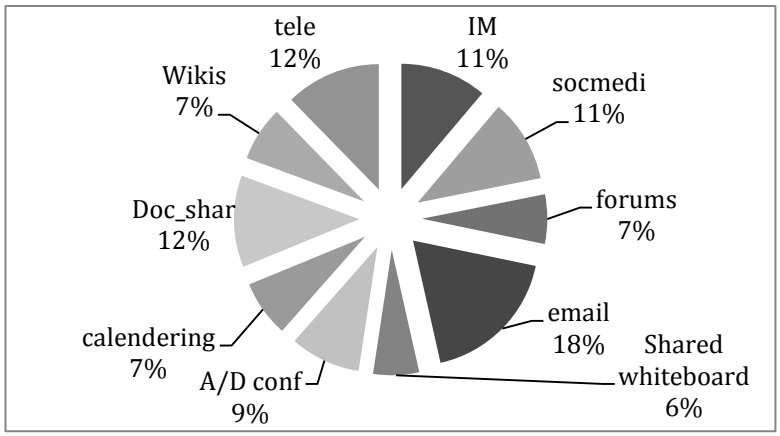


Figure 4.1: Students' perception of the security of the different OCG tools

It is notable that:

1- Only 8% of the respondents feel that IM and social media are ineffective, while 18% of the respondents think calendaring is an ineffective tool.
2- Nearly 30% of the respondents have not used most of the tools above.

B. Respondent's opinions of good authorization of OCG tools

Figure 4.2 illustrates the opinion of the respondents regarding authorization of CSCL tools. In the questionnaire, the respondents were asked to list three different CSCL tools that they think have good authorization. Out of 187 respondents, the majority – at about 20% – thought social media and email have good authorization whereas forums were selected by only 1% of the respondents.

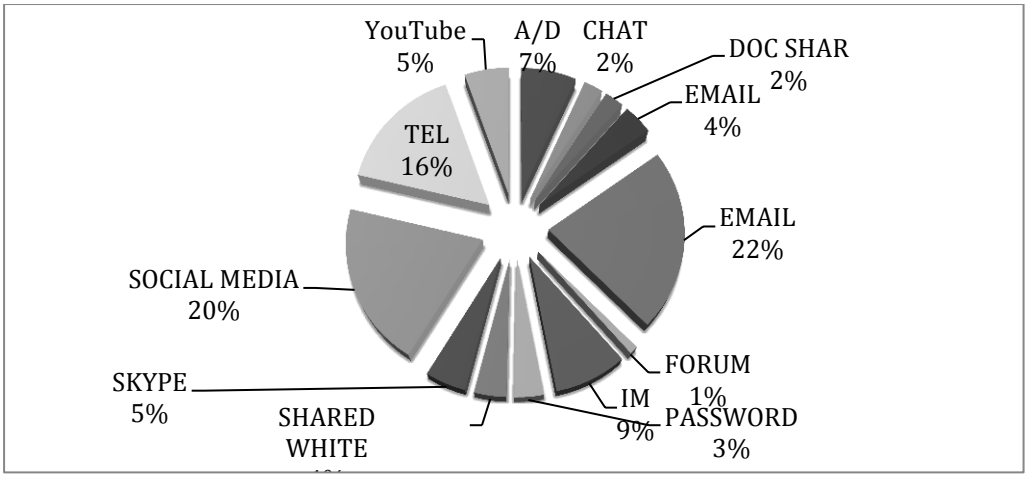


Figure 4.2: Respondent's opinions of good authorization of OCG tools

Similarly, Skype, shared documents, and passwords were also only picked as having good authorization by a noticeably small number of respondents (5%, 4%, 3% respectively).

C. Respondents' opinions of the poor authorization of CSCL tools

Figure 4.3 shows the opinion of respondents regarding the poor authorization of CSCL tools. In the questionnaire, the respondents were asked to list three different CSCL tools that they think have a poor authorization.

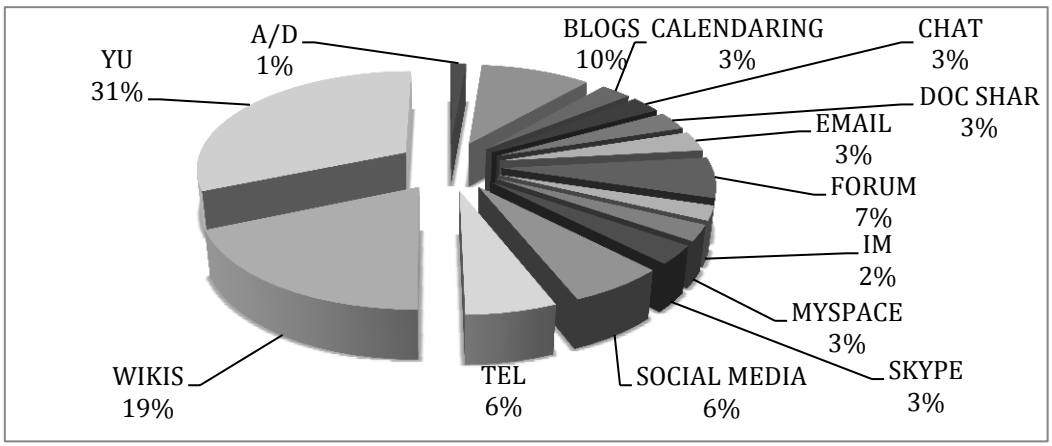


Figure 4.3: Respondents' opinions of the poor authorization of CSCL tools

Out of 187 respondents, the majority – at about 31% – thought YouTube has a poor authorization followed by wikis, which was selected as having poor authorization by 19% of the respondents.

It is shown in the chart that the tools Skype, MySpace, document sharing, and chat each have the same percentage of respondents that regard them as having poor authorization.

C. Security solutions software deployed in respondents' homes

The questionnaire respondents were asked to choose the security solution that they use at home.

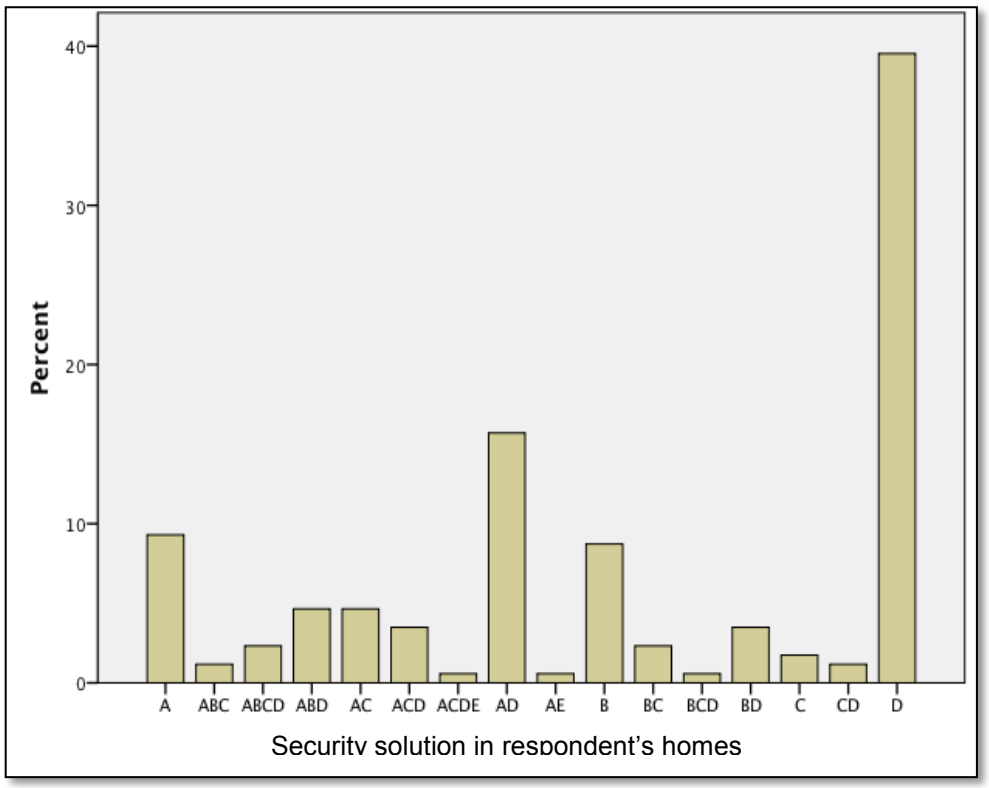


Figure 4.4: Security solutions software deployed in respondents' homes

There are 5 different security solutions in total, including Firewall (A), Antispyware (B),

Spam filter (C), Antivirus (D), and Other (E). It is clear from Figure 4.4 that the majority (37.2%) of the respondents use antivirus (D), while a few of the respondents stated that they use all of the security solutions in their home.

C. Security technologies familiar with respondents' environment The respondents were asked in the questionnaire to choose the security solutions that were familiar by the respondents. There were four options listed in the questionnaire including: Public/Private key (A), Biometrics (B), Protected Passwords (C) and Other (D).

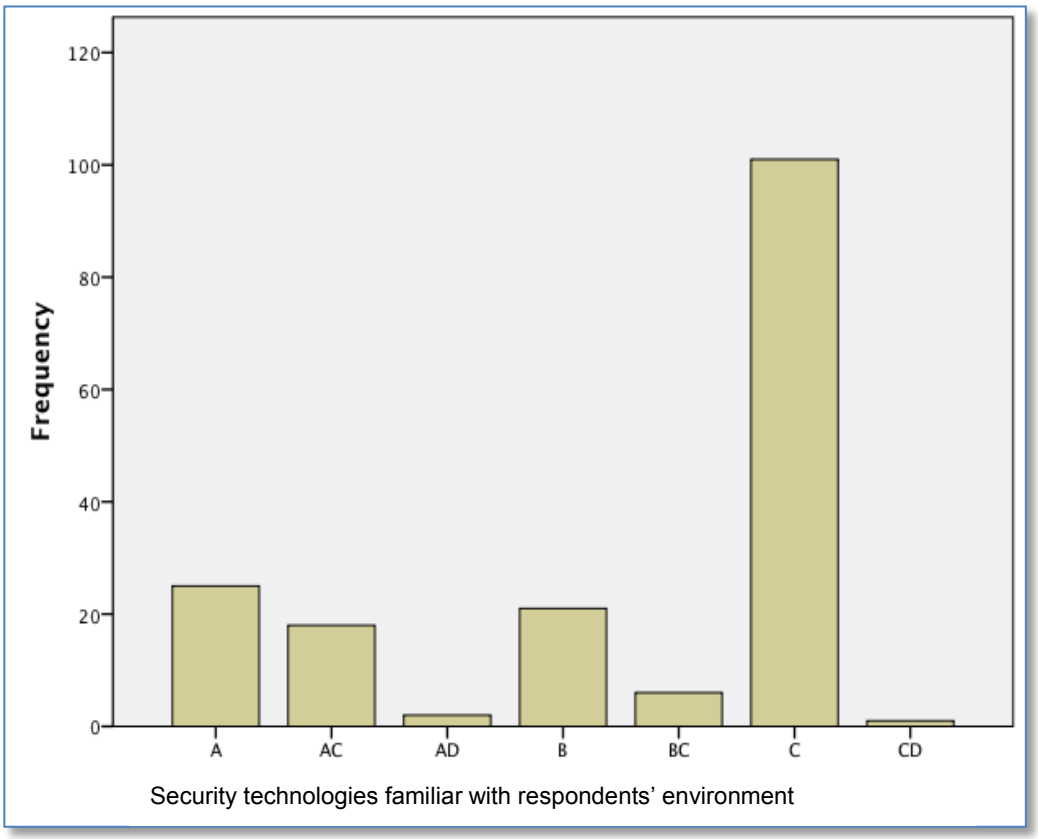


Figure 4.5: Security technologies familiar with respondents' environment

As is evident from the chart, the majority 100 (58.9%) of the respondents use passwords (C), while a small number stated that they use public keys (A).

D. Security technologies used by the respondents in their home environment.

Figure 4.6 shows the security technologies that are used by the respondents. Those surveyed were asked to choose the security technology that they used in their home from a choice of Public/Private key (A), Biometrics (B), Protected Passwords (C) and other (D). From the chart it is clear that a significant majority of the respondents 58.5% - chose C as the tool they were familiar with, while only a small minority were familiar with Biometrics (B) as a security technology.

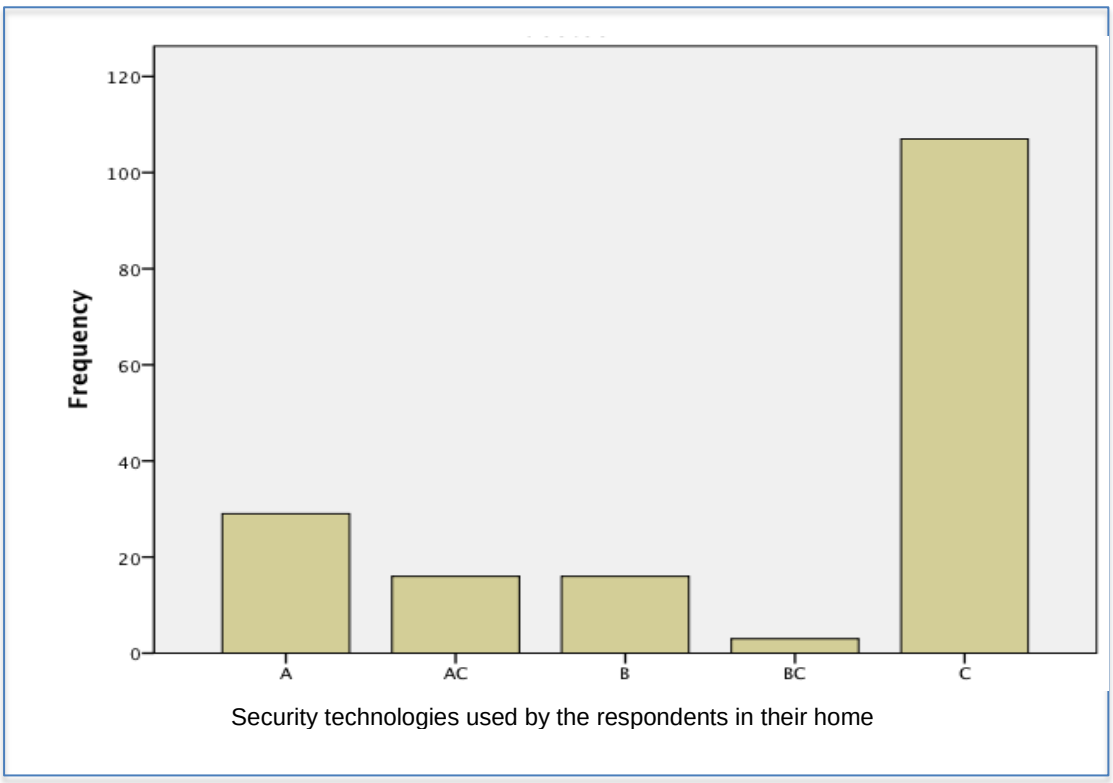


Figure 4.6: Security technologies used by the respondents in their home environment.

The respondents were asked about the types of information a teacher needs to preserve and with what level of access in order to deliver a course efficiently. There are six types including students' submitted assignments, shared whiteboard, and messaging history amongst others. For each one the respondents have to choose their preference from the following options:

- Private (A) means that the assignments are kept private and confidential to the administrator (and not available to the teacher).
- Access with permission from the user (B) means data is available to the teacher with the student's explicit permission.
- Preserved with permission from the user (C) means that data are available to the teacher but without any editing rights.
- Public (D) means data are visible to the teacher and all the students.

It is notable from Figures 1,2,3,4 (See Appendix G), that 39% of the total prefer their assignment answers to be private where as 9% of the total prefer them to be public. In addition to that, the majority (58%) preferred their grades, collaborative data (chatting between each other), and personal data (including age, course name, names, year of study) to be private.

4.3.2 Qualitative research methods

Interviews

Semi-structured Interviews were conducted to answer the research questions discussed in Chapter 3 with different students and teachers from the Information System (IS) department (See Appendix B) for the template used for the interviews. Interviews are useful in finding out participant's opinions regarding the difficulties and problems which cannot be measured by questionnaires only. The interviews highlighted some of important issues for the above research questions as some students claimed that they are scared of using OCG tools because of security, Others mentioned that using these tools waste their time.

Aims of the interviews

The researcher intended to conduct interviews with a sample of lecturers teaching IT

courses in the IT College at UOB, as well as with relevant students. The aim of these interviews was to pinpoint and extract the specific problems regarding the interviewees' perception of using OCG tools and the difficulties faced regarding security. Additionally, the interviews discovered their views on the use of OCG tools as a teaching and learning resource.

Design of the interviews

Interviews were conducted with 10 students and their teachers from different IT departments such as Computer Science, Computer Engineering, and Information system. Interviews were divided into three parts. Part 1 was an introduction, explaining the purpose of the interview. Part 2 dealt with the warm up section in order to pave the way for the students to join the interview. It consists of four questions about what they study, methods of studying, whether they use OCG tools in their learning and what kind of OCG tools. Part 3 consisted of cool-down questions as follows:

- Problems faced when using these OCG tools;
- Their perception and views towards these tools;
- Usage of these tools;
- Security problems faced while using these tools and what kind of problems;
- Suggestions to solve these problems in the learning.

Analysis of the teachers' interviews

In response to the question associated with "the problems have they faced when using these OCG tools", the interviewees' responses which are translated from the Arabic language are shown in the tables below.

Table 4.2: Problems faced when using these OCG tools

Code	Responses
T1	I, as a teacher, face a problem in that the students do not have awareness of using such tools. They use Facebook only with their friends.
T2	I, as a teacher, rarely use webmail in learning because the students are not motivated to use it. Most of them do not respond.
T3	I, as a teacher, face problems with security settings of the OCG tools.

Table 4.3: Teacher's perception and views towards these tools

Code	Responses
T1	I, as a teacher, use only Facebook and Twitter for friendship because they are easy to use.
T2	I, as a teacher, think such tools can be used in learning but students need awareness.
T3	I, as a teacher, think webmail usage is worthy whilst learning.

Table 4.4: Usage of OCG tools

Code	Responses
T1	I, as a teacher, I do not use Wiki and Twitter when learning. Sometimes I use email such as Hotmail with my colleagues.
T2	I, as a teacher, think emails are easy to use but Wikis and Skype are difficult.
T3	I, as a teacher, I use only e-learning platform such as blackboard. And I do not use its email even.

Table 4.5: Security problems faced while using these tools

Code	Responses
T1	I, as a teacher, do not trust webmail but I trust University email.
T2	I, as a teacher, do not know what kind of security problems you mean? I know that signing and encryption are difficult to set.
T3	I, as a teacher, know how to set the privacy of the Facebook and Hotmail security settings.

Table 4.6: Suggestions to solve these problems in the learning

Code	Responses
T1	The teachers and the students must have workshops to teach them how to use these tools in learning.
T2	Students must be encouraged by the teachers to use some of OCG tools that are familiar with in class.
T3	Students and teachers must be taught how to use the security settings provided by webmail.

Based on the above responses, it is clear that the teachers lack the awareness of using such tools in the learning. Moreover, the teachers complained that security settings provided by OCG tools are complicated. On the other hand, some of them know how to set the privacy of the Facebook and Twitter only. It is apparent from the above interviews that the teachers do not use other OCG tools such as Wikis and Skype because they are not familiar with them.

Analysis of the Students' interviews

The students' responses are similar and agreed each other. Therefore, I have chosen a representative selection of these responses which are shown in the tables below. In

respect of questions 1 regarding the problems faced when using these OCG tools; the responses of some students are shown in Table 4.7.

Table 4.7: problems faced when using these OCG tools

Code	Teacher's responses
S1	I, as a student, face a problem with technical issues
S2	I, as a student, think that webmail and Facebook expose me to hacker.
S3	I, as a student, feel anxiety when using webmail in the learning. I think it lack safety.
S4	I, as a student, do not believe in using email for learning

In respect of questions 2 regarding their perception and views towards these tools; the responses of some students are shown in Table 4.8.

Table 4.8: Their perception and views towards these tools

Code	Responses
S1	I, as a student, use only Facebook and Twitter in my social life.
S2	I, as a student, think that Facebook can support learning and can facilitate communication between the students and teachers.
S3	I, as a student, use Facebook and Twitter as social media with my friends only.
S4	I, as a student, do not feel comfortable when using webmail as I think it is not secure.

In response to the question associated with "Usage of OCG tools", some of the interviewees' responses are shown in Table 4.9.

Table 4.9:Usage of OCG tools

Code	Responses
S1	I, as a student, use Facebook but not for learning
S2	I, as a student, frequently use Facebook and rarely email but not for learning
S3	I, as a student, occasionally use only Facebook and forums but not for learning
S4	I, as a student, frequently use only Twitter and sometimes email but not for learning

In response to the question associated with "Security problems faced while using these tools" responses are shown in Table 4.10.

Table 4.10 Security Problems faced while using of these tools

Code	Responses
S1	I, as a student, do not know much information about security.
S2	I, as a student, do not trust any of these tools and always worried about my documents.
S3	I, as a student, think that they are not secured especially webmail.
S4	I, as a student, think most of them are secure.

In relation to the question associated with "suggestions to solve these problems in the learning" responses are shown in Tables below.

Table 4.11: Suggestions to solve these problems in the learning

Code	Responses
S1	I, as a student, suggest that the IT centre must prepare and solve all the security problems which lead us to trust them and then we can use it in the learning.
S2	I, as a student, suggest increasing the awareness of the usage and of OCG tools and it is the responsibility of the teachers to make students aware of the security issues.
S3	I, as a student, recommend using some of these tools for learning especially Twitter and Facebook
S4	I, as a student, recommend increasing the awareness of secure OCG tools amongst the teachers.

With reference to the students' interviews, it is clear that the students are only familiar with Facebook and Twitter and rarely use emails but they do not use them as learning tools. On the other hand, it seems that they are aware of the usage as they give suggestions to use it but they do not get encouragement from their teachers. With respect to security, it seems that the students do not know how to secure the OCG tools and may have some misconceptions about security. In conclusion, students need awareness and encouragement as well as trust in order to use the OCG tools.

Observations

It was observed from meeting the classes while the students were working that they are dependent and lazy – they do not want to try anything new. They prefer to use traditional methods for learning. Furthermore, the teachers do not make it compulsory (or even encourage) to use the new learning technologies such as OCG tools.

4.4 Conclusion

The teachers' and students' interview results indicate that the students and teachers lack knowledge of the security in some of the familiar OCG tools such as Facebook, Emails, Skype, and Twitter. They both commented that these tools waste teachers' and students' time as they are not familiar with them. In addition to that, they agreed that use of some of the common OCG tools such as Facebook and Twitter is worthwhile but they do not feel they have sufficient trust to use them. They feel anxiety when using webmail as they think it is exposed to hackers. It seems that the students do not trust such tools, and they do not feel comfortable when using them and always feel worried.

Overall, the initial research results signpost that lack of awareness and motivation and then trust are the key problems in OCG tools usage. The author proposes that these problems may be partially improved by a suitable environment in which aware teachers encourage students.

Based on the findings from the literature review, student questionnaire results and interviews with IT teachers and students, possible subject areas for using OCG tools in the learning:

- Increase motivation for the teachers and students;
- Raise awareness of secure OCG tools;
- Make the students and teachers aware of how to secure the OCG tools fundamentally.

Limitation

During the initial study including the survey and interviews, there has been some of limitations which constrained the activities and led to these results:

1- the participants are not motivated to response to the questionnaires and were not series to answer the questionnaires.

2- the participants did not have knowledge about some of OCG tools such as Skype

3- Some of the respondents did not read well the question of the questionnaire

4.5 Chapter Summary

The author proposes that the existing problems identified could be addressed with increase in awareness of the OCG tools, and that motivation for using the tools could be improved with the increase of trust. This is supported by the initial feedback from the students and teachers. These suggestions claimed by the author, in this context, are essential for teaching/learning to be effective and modern, in order to benefit the students.

The next Chapter will

- Critically find the students' perception of chosen OCG tools Such as Skype, Wiki, Facebook, and Gmail (SWFG);
- Gain a sense of how participants navigate through SWFG;
- Evaluate the security, safety, privacy and trust of SWFG tools and discover if there is a common behaviour for students during the experiment.

Chapter Five: Students' perception of secure SWFG tools

5.1 Introduction

In the previous Chapters, current problems in OCG tools usage were identified. Increasing security, safety, privacy, and trust which I refer to as (SSPT) can be a possible solution for the lack of OCG tools usage. To investigate this, the researcher chose to investigate the students' perception of particular chosen OCG tools such as Skype, Wiki, Facebook, Gmail (SWFG) during the learning process at UOB by conducting a quasi-experiment. In this experiment SWFG was evaluated to identify if they are secure, safe, private and trusted by the students. Following this experiment, some of these tools could then be further examined through evaluations and intervention activities in the next stages of this study. Before proceeding to the next section which explains the quasi-experiment, the meanings of the terms secure, private, safe and trusted SWFG tools should be clarified.

As discussed in Chapter 1, the following terms has been adapted for the purpose of this concept.

- Secure SWFG tools are the tools that have the tools' security settings enabled.
- Private SWFG tools have the ability for students to isolate information about themselves and thereby reveal themselves selectively.
- Safe SWFG tools are protected from harm such as viruses, spyware, etc.
- Trusted SWFG tools are tools that the students feel relaxed and at ease when using

5.2 Experimental Research Questions

The following questions are related to the two groups of students, the control group (A) and the experimental group (B), which were chosen as participants in the quasi-experiment.

RQ5.1: What are the differences between group A and group B in their perception of secure SWFG?

RQ5.2: What are the differences between group A and group B in their perception of safe SWFG?

RQ5.3: What are the differences between group A and group B in their perception of private SWFG?

RQ5.4: What are the differences between group A and group B in their perception of trusted SWFG?

RQ5.5: Are there any significant correlations between security, privacy, safety and trust, and usage of SWFG?

5.3 Hypotheses Testing

The researcher initially formulated four main hypotheses related to the tested groups A and B in order to answer the research questions 1 to 4. The main hypotheses are as follows:

Hypotheses:

H1: There are perceptional differences between group A and group B to the secure SWFG.

H2: There are perceptional differences between group A and group B on the safe SWFG.

H3: There are perceptional differences between group A and group B of the private SWFG.

H 4: There are perceptional differences between group A and group B of trusted SWFG.

Table: 5.1 Quasi-experiment design stages

Experiment's Stages	Data collection instrument	Data collection methods	Aim
1 A. Pre experiment Student Survey	Questionnaire	Quantitative	To find the students' perception of the Tested OCG tools.
1B.Pre-experiment Teachers/Students Interview	Interview	Qualitative	To establish if there is common feedback among teachers and to find the students' feedback
2. Keeping track of every action occurred with SWFG	Observation form Log files	Qualitative	To measure the differences among the groups. To discover if there is a common behavior for students during the experiment.
4.Post-experiment Students' Feedback	Questionnaire Observation	Quantitative Qualitative	To evaluate the SSPT of SWFG tools. Compare between the groups

In addition to these hypotheses, the researcher set another 23 hypotheses in order to answer the research question 5.5 and will be presented in detail in Table 5.10.

5.3 Methodology

In the present stage, a quasi-experiment was conducted to test our hypotheses.

The details of the quasi-experiment and the aims for each stage are summarized in the following sections, and depicted in Table 5.1.

5.4 Validation

Intended dimensions to be measured should be extracted from the theoretical perceptions of the dimensions that have to be measured. Therefore we needed to ensure the validity of the instrument, in that each item has to measure what it is intended to measure.

For this purpose, the researcher made a comprehensive review of previous attempts of measuring the variables that were treated in the present study.

A draft set of questions that has been included in the questionnaire was prepared. The researcher consulted a group of specialist referees consisting of 5 faculty members at University of Warwick, who were asked to give their opinion on the test items, to ensure the test questions reflected the content of security technologies with SWFG tools.

Additionally it was shown to 10 students at UOB to ensure their understandings of the questionnaire which will be discussed in the next section.

5.4.1 Triangulation methods

Triangulation is a combination of several research methods relating to the same study and it is often used to indicate that two (or more) methods are used in a study in order to ensure that each individual instrument gives similar. For this purpose, some of the interviews and observation have been applied in this experiment to validate the data.

5.5 Respondents

The participants were drawn from two undergraduate classes studying information systems at the Information Technology College in the University of Bahrain. These two classes were selected for logistical reasons since the researcher works at UOB. This allowed more accessibility to the students and aided the research procedures.

51 students aged 19-21 from two different classes at UOB were randomly selected as

participants in the experiment. The pilot respondents were discarded in the main study. Therefore, the questionnaire was administered to 51 students from two different classes so that the research can concentrate on each student while they access the tools during the experiment. The period of the experiment was one month.

5.5.1 Quantitative method

Quantitative data communicate meaning and interpret information by means of numerical analysis. This is accomplished by statistical methods that help to generalize findings. "Quantitative researchers adopt an objective stance regarding participants and their settings, and use sample research to apply their findings to a larger population" (Neuman, 2000; Dillman, 2000).

Questionnaire Survey

The researcher planned to conduct some questionnaire surveys at varying stages of the study. Those questionnaire surveys carried out with the students were conducted through a questionnaire distributed to the students in the classroom, both pre and post the test.

Upon validation, with some minor modifications and alterations to wording and technical aspects, the researcher distributed the questionnaire among the participants pre-test and post-test. Details of the design of this survey are described in following section.

Questionnaire survey 2-a

Questionnaire 2-a (See Appendix A) was distributed pre-test. It consisted of three main sections, including seven questions relating to personal information, experience of usage of SWFG, trust and security. Section one gathered demographic information about the participants, including age, year of study and education background. Section two, meanwhile, sought to collect information on the students' experience of SWFG and their

usage of SWFG when working on collaborative group work during their learning activities. Section 3 served to gather information about how the students felt when they used SWFG regarding trust, security, safety and privacy.

5.5.2 Construct of the instrument

Pilot testing

The case study tool was in the form of a questionnaire, and was presented to five external referees, who were faculty members from the Computer Science department at the University of Warwick. The referees were asked to read each question and to comment on questionnaire items in terms of wording and content, and to give their comments and suggestions for improving the scale.

Reliability

Pilot testing was conducted to test the reliability of section IV of questionnaire 2-b. The reason behind this is that section IV had 14 items on a Likert-like scale and the researcher needed this test to ascertain the internal consistency of all these items.

The researcher compiled responses from ten students to assess the reliability of the student feedback questionnaire.

The reliability confidence (Cronbach‘s Alpha) for the question in section IV of questionnaire 2-b was calculated. The value is to be regarded as being satisfactory (0.771), and is acceptable after items 4, 5, 6, 9, 10, 11 and 13 were deleted.

Explanation of each section of the questionnaire

1. The first section focused on obtaining the background of the target student respondents such as name, age, department, year of the study, course code, and their secondary school.

2. The second section focused on obtaining information about the respondents' experience of SWFG tools (such as Skype, Wikis, Gmail, and Facebook) as learning activities in home or university and types of activities like chatting, assignment submission, quizzes, and video conferencing. Finally, the respondents were asked about the frequency of their SWFG usage.

3. The questions in the third section aimed to measure the following:

- Students' trust, by asking them to express their feelings while they use SWFG tools based on a scale of (Afraid, Worried, Pleased and Motivated).
- Security, by asking the respondents which one of SWFG have more security based on a scale of (Very Secure, Secure, Neither Secure nor Unsecure, Unsecure, and Not Secure at All) using a Likert-scale (5-1)
- Safety, by asking respondents to express their thinking about which of the SWFG is more safe using a Likert scale (5-1) (Very Safe to Not at All safe)
- Privacy, using a Likert scale (5-1) (Has Strong Privacy – Has No Privacy at All).

This was followed by an open-ended question to investigate their willingness to use such tools in future.

Questionnaire survey 2-b

This questionnaire was distributed at the end of the experiment, and it was the same as questionnaire 2-a (See Appendix A) except that it has one more section (section 4) regarding motivation. The items are derived from the survey conducted by Dembovskaya (2009).The purpose of this section was to find out how often students were motivated while they used SWFG in the experiment. It consisted of 14 questions with 4-point Likert scales as shown in Table 5-2.

Table 5.2: Likert scale for questions in section 4

Scale	Description
1	**Not true**
2	**Somewhat true**
3	**True**
4	**Very true**

5.6 Experiment design

The researcher used a mixed-model design for the test, combining quantitative and qualitative methods. Regarding the quantitative methods, the researcher followed a quasi-experimental design. The researcher conducted the experiment with two groups. The control group did not set the security techniques with their emails and the other ('experimental') group was working with the secure email. Both groups were assessed pre and post the experiment. The students in both groups were given a project to work with and assignments (See Appendix D). The experiment design, along with the data collection techniques, will be discussed below.

At the beginning of the first semester, in October 2012, two classes of 51 undergraduate students in the IS department of the IT college were chosen as participants; each class was divided into two groups, control group A and experimental group B.

The security, safety, privacy and trust of the SWFG selected were critically evaluated by the researcher, and studied on the basis of the factors depicted in Table 5.1, for which a triangulation method was adopted and applied to aid comparison.

Table 5.3: Security mechanisms of SWFG

Learning activities	OCG tools	Security mechanisms	Details
Real-time data conferencing, electronic display, video conferencing and audio conferencing)	Skype	Authentication and Authorization	See Appendix C
Assignment submission	Gmail	Verification	See Appendix C
Chatting/discussion/ idea generation	Wikis	Authentication and Authorization	See Appendix C
Chatting/discussion/ idea generation	Facebook	Authentication, authorization	See Appendix C

"Authentication is used to ensure that the entity requesting access to the system is what or who it claims to be while authorization to allow access only to those resources which are appropriate to that entity's identity." (buisnessdictionary, 2014)

SWFG model

The researcher has developed a SWFG model as shown in Figure 5.1. The aim of the SWFG model is to allow the students to use SWFG in their learning during the experiment. It includes Skype, Gmail, Facebook, and Wikispace (SWFG) tools with interrelationship according to their purposes in the experiment.

Details of the learning activities with the security settings are shown in Table 5.3

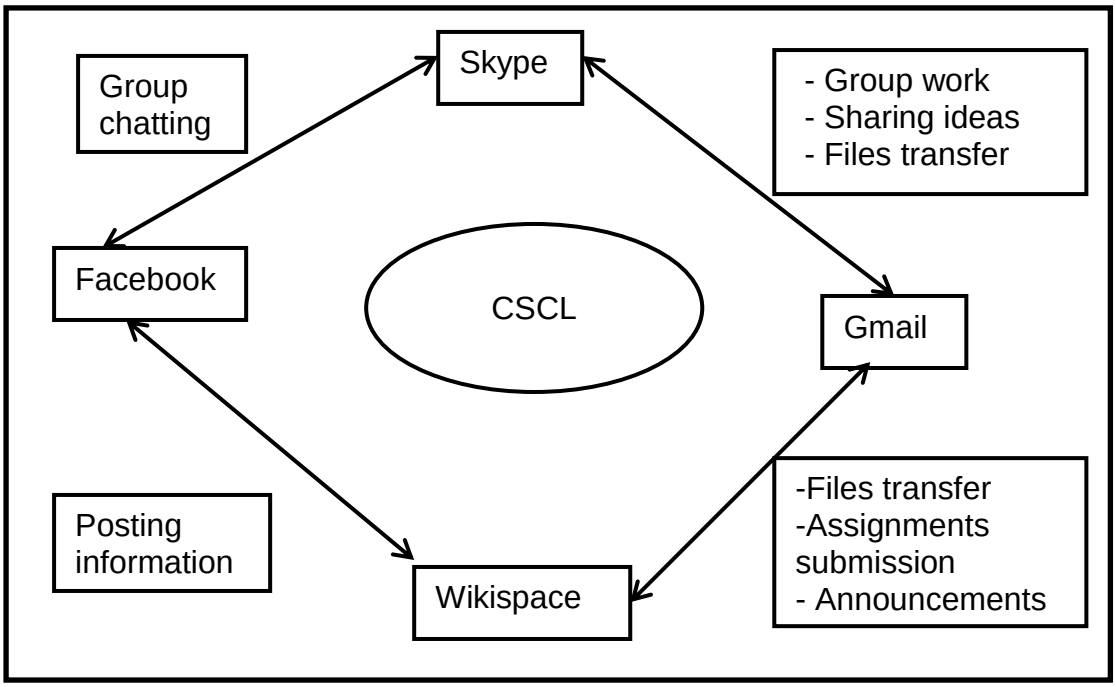


Figure 5.1: SWFG model

SWFG model:

As shown in Figure 5.1, the participants in both groups A and B were allowed to use the following SWFG tools during the experiment (See Appendix C).

Skype: Each participant has signed in with a new account in Skype and added the other participants in the groups.

Wiki: The participants have created their own wikis and invited each other in the groups to share their ideas.

Facebook: Most the participants have a Facebook account so they were allowed to create a group with the name of the course. Also, they invited each other to share the course contents, assignments and opinions.

Gmail: The participants have signed into a new Gmail account with the course name account.

Experiment activities

Two assignments were chosen as a means of evaluating the usage of SWFG in the case study (See Appendix D) within a period of four weeks. The quasi-experiment contained the following activities:

Stage 1: A questionnaire survey 2-a and interviews with students were conducted before the start of each assignment (See Appendix A),

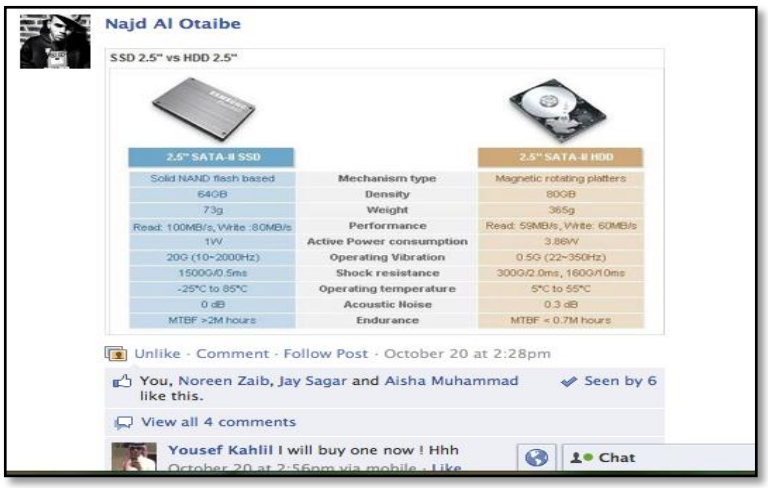


Figure 5.2: Screen shot of sharing information via Facebook

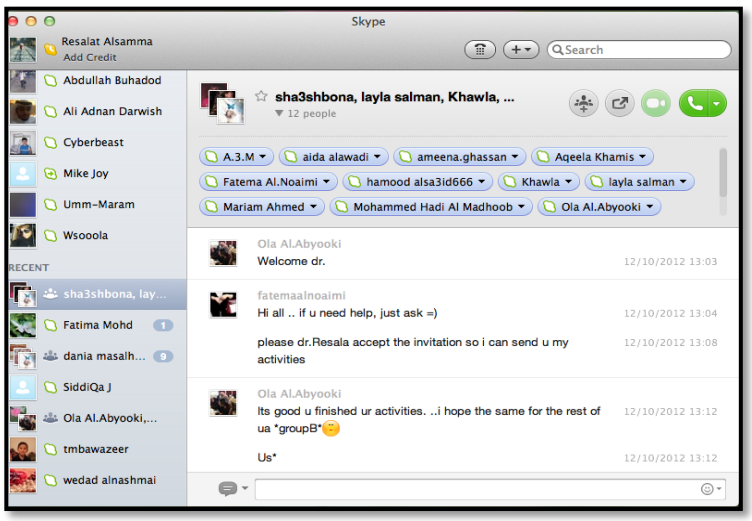


Figure 5.3: Screen shot of group chatting using Skype

Stage 2: Both groups from both classes started their assignments using SWFG, and the experiment started as follows:

Group A from each class used the SWFG without setting their security and privacy.

Group B used the SWFG in security mode, as depicted in Table 5.3 and Appendix C.

After group B had set the security settings for the SWFG tools, both groups undertook the following learning activities:

1. Both groups edited the wikis and answered question 1 of Assignment 1 (See Appendix D).
2. They shared information with other students in the same group and their teachers, and also used Facebook to share pictures, ideas and information related to the assignment, as depicted in Figure 5.2.
3. They transferred files using Skype and Gmail. They chatted with each other and with their teacher during the day as depicted in Figure 5.3.

Stage 3: The assignment was submitted using one of the tested SWFGs. Following this, questionnaire 2-b (See Appendix A), was distributed among the participants.

The research methods were applied as will be discussed in the following section.

5.7 Data Analysis Methods

Descriptive statistics were applied to gather four aspects of information from the responses to the survey: (i) demographic information on the participants; (ii) students' experiences of OCG tools; (iii) information on the types of personal feelings that the students had previously when working on online group work during learning activities; and (iv) information about the students' motivation whilst using SWFG during the experiment.

5.7.1 Participants' demographic information for groups A and B Pre test

All 51 students answered questionnaire 2-a,Table 5.4 shows that many of whom (27.5% of the total) were students from Manama city, the capital of Bahrain, which contains more educated people than the other areas.

Table 5.4: Different geographical areas of the participants (valid responses)

Area in Bahrain	**Frequency**	**Percent**
Hamad Town	7	13.7
Isa Town	10	19.6
Jidhafs	3	5.9
Manama	14	27.5
Muharaq	6	11.8
Riffa	4	7.8
Saar	4	7.8
Saudi school	1	2.0
Sitra	2	3.9
Total	*51*	*100.0*

Additionally, 13.7% were students from Hamad town, a modern town with people from many cultures. It has one of the best modern schools and has well developed technology tools and smart boards. Following these were students of Muhraq (11.8%). Muharq is the second modern city in Bahrain, and has well developed schools. However, only 2% and 3% of the total were students from Sitra and Jidhafs villages, respectively.

These results show that the sample consists of highly educated students who had

familiarity with new information and communication technology (ICT). This can help the researcher to progress in the case study.

5.7.2 Experience using SWFG

Q3 in the questionnaire 2-a asked the participants of both groups A and B about their experiences with SWFG usage at home and at the University as follows: (See Appendix A).

Experience using Gmail

The participants were asked about their experience of Gmail at home and at the university.

Table 5.5: Places of Gmail usage

		Frequency	Percent	Valid Percent
Valid	Home	25	49.0	50.0
	Home/University	21	41.2	42.0
	University	4	7.8	8.0
	Total	50	98.0	100.0
Not used on either university nor home		1	2.0	
Total		51	100.0	

As shown in Table 5.5, 49% of the participants used Gmail at home, whereas only 7.8% used Gmail as a collaborative tool in the university. Only one student commented that he/she had not used Gmail either at the university or at home. This may be because he/she used another kind of email. Overall, these statistics indicated that the majority of students were proficient in their use of Gmail. This result shows that the experiment for

using Gmail proved to be straightforward for the participants.

Experience using Facebook

As shown in Table 5.6, 60.8% of the participants had experienced using Facebook at home and about 23.5% of the students had experienced using Facebook at university. Additionally, only 8 participants did not use it either in the university or at home.

These figures show that the majority of participants aware of Facebook usage in the learning. This indicated a high confidence for obtaining good results, facilitating the conducting of the experiment – particularly with respect to the internet and social network aspects of the experiment.

Table 5.6: Places of Facebook usage

		Frequency	Percent	Valid Percent
	Home	31	60.8	72.1
	Home/University	31	23.5	27.9
	Total	43	84.3	100.0
Not used on either university nor home		8	15.7	
Total		51	43	

Experience using Wikis

As depicted in Table 5.7, 15.7% of the participants had experienced using Wikis at home. However, about 4% of the students had experience with using Wikis in the University, or both. It may be seen that 76.5% of participants answered that they did not

use the tool either in the university or home. It is clearly shown that the majority did not use Wikis, and this means that they have do not have enough background experience of using this tool in learning.

Table 5.7: Places of Wiki usage

		Frequency	Percent	Valid Percent
Valid	Home	8	15.7	66.7
	Home/University	2	3.9	16.7
	University	2	3.9	16.7
	Total	12	23.5	100.0
Not used on either university nor home		39	76.5	
Total		51	100.0	

The interviews (featuring 6 students) supported this result. As the student S2 stated "I don't know how can I use Wikis in learning…. I know that I can use Wikis for getting information."

Experience using Skype

As shown in Table 5.8, 41.2% of respondents used Skype for learning activities at home, whereas only 5.9% of the participants chose Skype in University.

Most of the participants (52.9%) did not use Skype as a learning tool in the university or home. Thus, the majority did not have any familiarity with Skype.

Table 5.8: Places of Skype usage

		Frequency	Percent	Valid Percent
Valid	Home	21	41.2	87.5
	University	3	5.9	12.5
	Total	24	47.1	100.0
Not used on either university nor home		27	52.9	
Total		51	100.0	

5.7.3 Comparison between daily' usage of SWFG pre- and post-test

As shown in Table 5.9, 78% and 56.9 % of the total participants had not used wikis and Skype respectively pre-test. On the other hand, only 12.5% and 4.8% of the total participants respectively had not used them post-experiment.

Numerous differences may be seen between the usage of these tools pre and post- test. In addition to this, there was a significant increase in the percentage of the participants who use Facebook, Gmail, and Skype for greater than 2 hours after the test (31.8%, 75.6%, 33.3% respectively) compared to pre-test (29.2%, 15.7%, 7.8% respectively). This means that they use SWFG tools efficiently and daily, which confirms the result of the experiment and supports the hypotheses.

Table 5.9: Daily usage of OCG tools Pre- and post-test (valid percentage)

OCG tools	I do not use it		<1 hr		>=1 but <2 hrs		> 2 hrs	
	Pre	Post	Pre	Post	Pre	Post	Pre	Post
FB	8.3	2.3	29.2	25.9	33.3	40.9	29.2	31.8
Wikis	78.0	12.5	8.0	55.0	10.0	25.0	4.0	7.5
Gmail	7.8	13.3	49.0	44.4	27.5	17.8	15.7	75.6
Skype	56.9	4.8	23.5	31.0	11.8	31.0	7.8	33.3

5.7.4 Comparisons between Group A and B in terms of their motivation (post-test)

The researcher has asked the participants about their motivation post-test in the questionnaire 2-b (section IV). Table 5.10 shows the data of the participants' perceptions of the different kinds of motivation items. These items measure the students' motivation after doing the experiment for both groups A and B.

It is clearly depicted that there are obvious differences between group A (who use unsecure SWFG tools) and group B (who use secure SWFG tools) regarding their motivation with respect to 'satisfaction with performance' and 'Aspiration'. 17.9% and 42.9% of group B reported 'Very True' and 'True' respectively, with regards to 'aspiration' while using SWFG tools in the experiment. 46.4% and 35.7% of group B were satisfied or very satisfied with their performance.

With respect to self-esteem, interest, satisfaction, and willingness there are minor differences which indicates that students in group B have motivation to use SWFG, regardless of the security. On the other hand, there were no large differences between group A and B when the considering competence and SWFG value.

Table 5.10: Motivation of the participants (valid percentage)

Motivation items	Item 1 Self esteem		Item 2 SWFG value		Item 3 Interesting		Item 7 Competence		Item 8 Satisfaction with Performance		Item 12 Aspiration		Item 14 Willingness	
Groups	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**
Not true	9.1	7.1	9.1	0	18.2	3.6	18.2	3.2	9.1	0	18.2	14.3	0	3.6
Somewhat true	9.1	25	0	14.3	18.2	14.3	27.3	32.1	36.4	17.9	36.4	25	27.3	14.3
true	45.5	25	36.4	39.3	9.1	25	27.3	46.4	36.4	46.4	18.2	17.9	9.1	14.3
Very true	36.4	42.9	54.5	46.4	54.5	57.1	27.3	17.9	1.28	35.7	27.3	42.9	63.6	67.9

This means that group A believes that SWFG tools have value after doing the experiment. Therefore, secure SWFG are not necessary for achieving competence and believing in their values.

5.8 Hypotheses testing results

The security, safety, privacy and trust of SWFG were measured using a t-test for both groups A and B at the post-test stage. Normality is assumed as the sample size is >=30.

"The t distribution provides a good way to perform one sample tests on the mean when the population variance is not known provided the population is normal or the sample is sufficiently large" (Zaiontz, 2014).

The researcher used SPSS software to calculate the result of the t-test (See Appendix D). The results of the questionnaires analysis and hypotheses result for security, safety, privacy and trust are as follows:

5.8.1 Security

Both group A and B answered question 5 of the questionnaire 2-b. The question was related to secure email (See Appendix A).

Table 5.11: Independent samples t-test

SWFG tools	T	df	P
Gmail	-0.397	47	0.693
Facebook	-0.048	44	0.962
Wikis	1.074	10	0.308
Skype	1.099	25	0.282

Table 5.11 shows the hypothesis 1.1, 1.2, 1.3 and 1.4 which predicts that there are differences between group A and group B in their perception of the security when using Gmail, Facebook, Wikis, and Skype are rejected (P>.05).

5.8.2 Safety

Data analysis of the t-test of question 6 of questionnaire 2-b which measured the safety of the SWFG for both groups A and B during learning, revealed the following:

Table 5.12: Independent samples t-test

SWFG tools	T	df	P
Gmail	-1.590	46	0.119
Facebook	0.32	47	0.974
Wikis	-1.871	7	0.104
Skype	1.124	5.78	0.307

Hence, the hypothesis 2.1, 2.2, 2.3 and 2.3 which state that there are differences between group A and group B in their perception of the safety when using Gmail, Facebook, Wikis, and Skype are rejected.

5.8.3 Privacy

Data analyses using the t-test, question 7 of questionnaire 2-b which measured the privacy of the SWFG during learning are shown in Table 5.13.

Table 5.13: Independent samples t-test

SWFG tools	t	df	P
Gmail	0.454	48	0.652
Facebook	0.538	44	0.593
Wikis	0.893	6	0.406
Skype	2.461	20	0.023

Referring to Table 5.13, it is demonstrated that H3.2, H3.3 and H3.4 (which state that there are differences between A and B in their perception of privacy when using Facebook, Gmail, and Wikis) are rejected (P>0.05). However, H3.1 which supposed that there are differences between group A and group B in their perception of the privacy when using Skype is accepted (P<0.05).

5.8.4 Trust

Data analysis using the t-test of question 4 of questionnaire 2-b which measured the trust of the SWFG during learning are summarized in Table 5.14.

It is clear from the Table (P>0.05) that hypotheses 4.1,4.2,4.3,and 4.4 which stated that there are differences between group A and group B in their perception of the trust when using the SWFG tools are rejected.

Table 5.14: Independent samples t-test

SWFG tools	T	df	P
Gmail	-0.216	46	0.830
Facebook	-1.112	43	0.272
Wikis	0.098	9	0.924
Skype	-1.129	16.952	0.404

Furthermore, based on the previous result, the researcher tested the research hypotheses with group B participants after the experiment in order to answer the research questions 5.5.

The hypotheses were checked by bivariate correlations method using SPSS software.

The Table 5.15 shows these hypotheses and whether they were accepted**.**

Hypotheses 1,3, 5, and 6 were accepted, but with a negative correlation as follows:

1- Secure Gmail has a significant negative relationship with Gmail usage.

2- Secure wikis has a significant negative relationship with wiki usage

3- Secure Gmail has a significant negative relationship with trusting Gmail

4- Secure Facebook has a significant negative relationship with trusting Facebook.

5- This means that the researcher cannot confirm these hypotheses for the research.

6- On the other hand, the rest of the hypotheses shown in the table above are rejected.

Table 5.15: Details of the research hypotheses tested

No	Hypotheses	Pearson correlation	(P)-value
1	Secure Gmail is significantly related to Gmail usage	-0.535	0.003 sig at P<0.001
2	Secure Facebook is significantly related to Facebook usage	0.162	0.409 P>0.05
3	Secure wikis is significantly related to wiki usage	-0.422	0.032 sig at P<0.05
4	Secure Skype is significantly related to Skype usage	0.000	1.00 P>0.05
5	Secure Gmail is significantly related to trusting Gmail	-0.568	0.002 sig at P<0.001
6	Secure Facebook is significantly related to trusting Facebook	-0.419	0.030 sig at P<0.05
7	Secure wikis is significantly related to trusting Wikis	0.040	0.853 P >0.05
8	Secure Skype is significantly related to trust in Skype	-0.0226	0.248 P>0.05
9	Safe Gmail is significantly related to trusting email	-0.370	0.057 P>0.05
10	Safe Facebook is significantly related to trusting Facebook	-0.203	0.310 P>0.05
11	Safe wikis is significantly related to trusting wikis	-0.037	0.863 P>0.05
12	Safe Skype is significantly related to trusting Skype	0.082	0.705 P>0.05
13	Private email is significantly related to trust in email	-0.302	0.126 P>0.05
14	Private Facebook is significantly related to trust in Facebook	-0.376	0.053 P>0.05
15	Private wikis is significantly related to trust in wikis	-0.275	0.194 P>0.05
16	Private Skype is significantly related to trusting Skype	0.020	0.920 P>0.05
17	Trust in email is significantly related to email usage	0.274	0.167 P>0.05
18	Trusting Facebook is significantly related to Facebook usage	-0.216	0.279 P>0.05
19	Trusting wikis is significantly related to wikis usage	-01.91	0.351 P>0.05
20	Trusting Skype is significantly related to Skype usage	-0.040	0.843 P>0.05

5.8.5 Qualitative data

In this study, the researcher employed qualitative data methods for pre- and post-experiment to conduct interviews with seven randomly selected students and two teachers in the information system at UOB. In addition to the questionnaire, recorded observations and log files have been used to provide further confirmation to the results.

The aim of these interviews was to pinpoint and extract the specific problems with regards to the difficulties and problems faced by lecturers and students. It also aimed to get their views on the use of SWFG as a teaching and learning resource (See Appendix B).

A. Pre-test:

Design of the interview

The semi-structured interview was divided in to three parts as follows:

1) Introduction about my interviews

This part aimed to introduce the interviewees to the researcher and to describe the aim of the interviews.

Warm-up period:

This section has 5 questions related to their study and their experience in SWFG usage as follows:

1. What are you studying?
2. How do you usually study?
3. Have you ever used communication tools in your study like Facebook?
4. Have you heard about collaborative groupware learning tools?
5. What are these?

1) Cool-down period:

This section has 4 questions about their perception in using SWFG and what kinds of problems they faced during accessing SWFG as the following:

1. What are the problems have you faced when using these tools?
2. Have you faced security problems? What are these?
3. What are your suggestions to solve such problems?
4. Would you like to continue using these tools in your learning? Why?

Faculty members' views

The responses of the two faculty members were as follows:

1- We did not use any of the SWFG in the learning;

2- We do not know that Skype can be used in the learning;

3- The UOB strategy does not encourage us to deal with these tools and we could get benefit from these tools if we use them as learning assistance tools.

Interviewees views

The responses of the IS students were as follows:

1- S1 pointed out that "We know these tools, particularly Facebook, but we don't imagine that we can utilize such a tool in the learning…";

2- S2 stated that they had not used these tools in the learning and "I don't think we can use them because we do not have time."

3- S3, S4, S5 and S6 said that "We don't trust tools such as these… also the teachers do not motivate us to use them"

4- S7 commented that "I am so interested to use them."

Observations

The researcher has recorded some observation points at the beginning of the experiment and during the experiment as follows:

- Participants were panicked and confused;
- It took time to access Gmail, especially group B when they started to fix the security settings for SWFG.

B. Post-test:

The interview was conducted after the experiment with the interviewees from group A and group B.

Design of the interview

The post-experiment interview was divided in to two parts as follows:

1. **Warm-up period:**
    - In which group were you working?
    - Which SWFG have you used more?
2. **Cool-down period:**

- What problems have you faced whilst using these tools?
- Have you faced security problems? What are these?
- Do you trust these tools after setting the security?
- How frequently did you use these tools?
- Would you like to continue using these tools in your learning? Why?

Faculty members' views

The same previous faculty members were asked about their perception towards the usage of these tools in the learning and their responses are as follows:

F1 pointed out that this is very interesting "I used SWFG and I will use Facebook and Skype in the learning and I already joined some of the students in Facebook during the experiment". Another faculty member pointed out "I cannot believe what I observed,

most of group B students join the Facebook and send me comments and share the assignment information". On the other hand, F2 did not like any tool and she said "we will try in the future but I do not think the students will accept them because they cannot believe what they post and feel comfortable with ease when they work with it them…"

Interviewees' views

Group A:

The responses of the interviewees of group A were as follows:

- GA1 commented that "the usage of Skype and Facebook was valuable and I enjoyed communicating with other students by the Skype". Other participants claimed that "the Gmail was not useful as we cannot trust it"
- GA2 commented, "We cannot imagine how these SWFG can facilitate our learning process, Skype shortens the way between us as students and strengthens the relationship between the teacher and us".

-The interviews with students revealed that many of the students were familiar with Facebook as the student GA3 pointed out "We are using Facebook to share information with my friends but I do know that I can use it as a tool in learning".

Group B:

Group B were interviewed and the following are their comments:

- GB1 commented that "after fixing the security settings for SWFG I can trust and enjoy using it"
- Most of group B claimed we feel little panic when we fixed security settings in the Gmail.
- GB2, GB3, and GB 4 pointed out that "We faced difficulties during fixing and usage of the security settings for Wiki. We think we need more practice in using

it”

- GB5 claimed “We really enjoyed using Skype and Facebook in the learning, I wish to use them further in the learning.”

Observations during the experiment

The researcher did not notice any difference between group A and B when they accessed Gmail. On the other hand, it was noticed that group B accessed Facebook with self-confidence and motivation. There were no differences between groups A and B when they used Wiki and Skype as both groups were interested in using Skype and more frustrated when they used Wiki. The interviewees were very active.

Log files

Furthermore, log files during the experiment support these conclusions. Log files here refer to the chat and communication history of the participants during the experiment for SWFG tools.

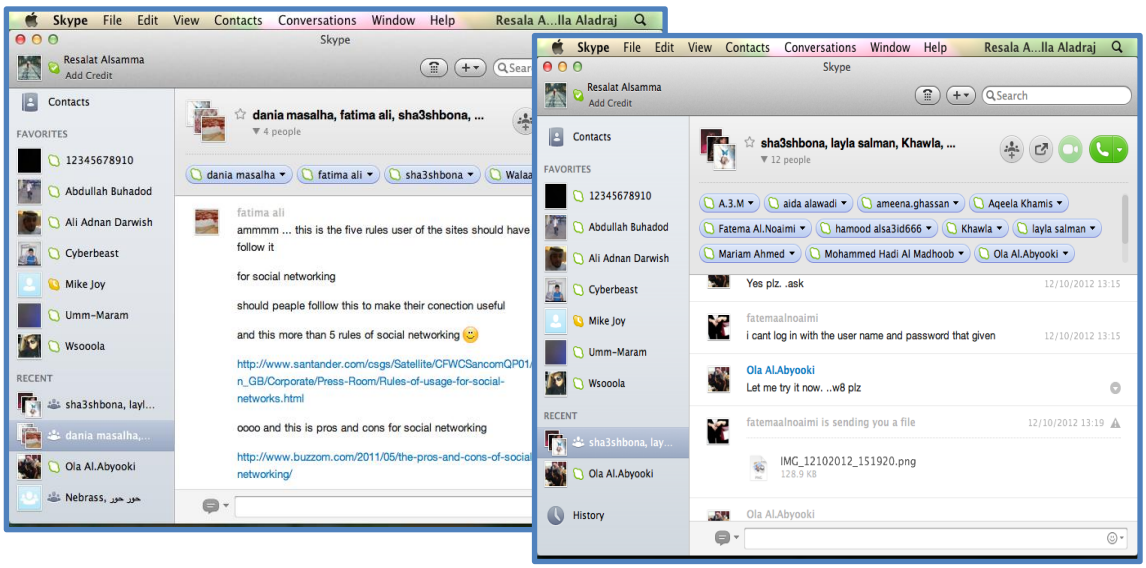


Figure: 5.4: Screenshots of the Skype conversations between participants

This history may be taken as support for the t-test result and emphasizes the comments made in the interviews.

The researcher had interviews with some of them and took their points into consideration.

The following are the main points checked:

1- Date of access
2- Reason for access
3- Number of group members
4- Number of times they accessed the tools.
5- Which tools were more frequently accessed.

The researcher has perceived that the most frequently accessed tools were Skype and Facebook, which they used to chat with the other students in the same group, and shared the assignments with the researcher and each other. With regards to Facebook, the majorities of the participants were active with Facebook as they shared posts with the researcher, and shared the assignments' answers with each other and the researcher. Figure 5.2 shows a screen shot of posting information of one of the participant.

5.9 Discussions and Conclusions

The aim of this activity is to identify and understand the perception of the students towards security, privacy, safety and usage of SWFG in the learning at University of Bahrain. The findings of this investigation, together with hypotheses testing, have enabled the researcher to succeed in this aim.

The overall finding of this activity is that there are no differences between groups A and B when using SWFG tools in terms of security, safety, trust and privacy. However there

are differences between groups A and B in terms of privacy when considering Skype usage. These results provide evidence that the participants (particularly group B) were not aware of the SSPT techniques, and their perceptions of SSPT with SWFG were the same as group A. Furthermore, the researcher has conducted a correlation test in order to identify whether there is a correlation between the usage and trust of SWFG tools and the use of settings for privacy, security, and safety. Based on the Table 5.14, the researcher has drawn the following conclusions, summarized as the following:

1- Secure Gmail has a significant negative relationship with Gmail usage.
2- Secure wikis has a significant negative relationship with wiki usage
3- Secure Gmail has a significant negative relationship with trusting Gmail
4- Secure Facebook has a significant negative relationship with trusting Facebook.

From the previous results, it is clear that secure Gmail, Wikis and Facebook have a negative correlation between their usage and trust. This result confirms the results of the hypotheses discussed above in relation to Gmail, Wikis and Facebook in that the participants were not aware of the security and it did not affect their usage of these tools. However, there is no correlation between any of other SWFG tools which are shown in Table 5.10 when they are secure, private, and safe.

On the other hand, it may be seen in Table 5.9 that most of the participants did not use Wikis and Skype pre-test and there was a significant increase in the percentage of participants using Facebook, Wikis, Gmail ,and Skype, at the post- experiment stage (31.8%, 7.5% , 75.6%, and 33.3% respectively). These results provide evidence that there was an improvement in SWFG tools usage at the post experiment stage. Moreover, Table 5.9 confirms the descriptive results which show that there are clear differences between group A (who use unsecure SWFG tools) and group B (who use secure SWFG

tools) regarding their motivation with respect to ‘satisfaction with performance’ and ‘Aspiration’. This means that students in group B have motivation to use SWFG regardless of the security. There is a conflict between this correlation and the descriptive results shown in Table 5.9 and Table 5.10. In addition to that, observations, log files, and interviews confirm the results, showing that the participants were active, inspired and motivated during the experiment. GB1 supported this by saying “the usage of Skype and Facebook was valuable” and she “enjoyed communicating with other students by the Skype”

There have been several limitations during the experiment as follows:

- First of all, the research was only conducted at the University of Bahrain (UOB), whereas including other universities in Bahrain might provide a better representation of Bahraini students. This would have enabled the researcher to work towards more comprehensive findings, representative of students all over Bahrain;
- Furthermore, only first-year students aged (19-20) at UOB participated in this study. A wider study would comprise students of different stages of their studies;
- A further limitation of the study may be the validity and reliability of the investigations conducted, and the lack of participants’ credibility when they answer the questionnaire. However, the researcher has attempted to minimize the impact of this investigation by using multiple methods of data collection to complete this study. For example, interviews, log files and observations were widely used throughout to ensure that data was collected from different sources**;**
- Lack of the participants’ awareness about SWFG and SSPT during the experiment.
- During the experiment, the participants gained knowledge about SWFG and

therefore their usage were increased;

- Lack of the participants responding to questionnaires and interviews.

Thus, the researcher will focus and concentrate her study on the security and trust of Gmail only, because since June 5, 2012, email has a new security feature which was introduced to protect users from state-sponsored attacks. Additionally, emails have a large user base compared to other OCG tools. Therefore, email can be chosen as an investigation tool in my research.

The investigation of email usage and trust amongst the students in UOB and the UK, and their awareness of these techniques will be discussed in Chapters 6, 7 and 8.

5.10 Chapter summary

The main results of this experiment have been translated into actionable suggestions to be implemented. The study has demonstrated that implementing secure SWFG provides a suitable solution to the lack of collaborative group work in the classroom environment, and can help to motivate the students to trust OCG tools, increase trust in such tools, whilst assisting in the teaching of difficult technical knowledge in a more efficient and practical manner.

Based on the above results, the researcher will conduct an intervention in order to test the security, trust, and usage of emails. This will involve a further consideration of the security that affects the usage and trust of emails. Chapter 6 will evaluate the students' awareness of secure email usage.

Chapter Six: Evaluation of the secure email awareness

6.1 Introduction

Based on the results of the quasi-experiment discussed in Chapter 5 which indicated that students were not aware of SWFG tools and do not trust such tools the aim of this Chapter is to reveal the students' awareness of such tools when they access email with security settings enabled. In doing so, the researcher has conducted a survey with the students in Bahrain and in the UK to achieve the aim.

6.2 Research questions

This activity was carried out in order to answer the following research question:

RQ 6.1: How (and how much) students are aware of secure email used and delivered to support group collaboration?

- RQ 6.1.1. What are the most frequent webmail/application email programs used by students in Bahrain and the UK?
- RQ 6.1.2. How often do the students access their email?
- RQ 6.1.3. How secure do students perceive their email to be?
- RQ 6.1.4 How secure do the students feel when using their frequently accessed email?
- RQ 6.1.5 How often do students use signing and encrypting of email?
- RQ 6.1.6 How aware are the students of secure email settings when they access email in general/with families and friends/important members of an institution?
- RQ 6.1.7 Do the students understand the importance of secure email?
- RQ 6.1.8 What are the differences in students' awareness of secure email between Bahrain and the UK?

6.3 Hypotheses

The researcher has established the following hypotheses in order to address some research questions, while others were answered by descriptive data, as shown in the Table 6.1.

The population is referred to the students at Warwick University or Coventry University in UK and University of Bahrain or the Arab Open University.

The sample is referred to 200 from Warwick University and Coventry University in UK and 200 from either University of Bahrain or the Arab Open University

It is supposed by the statistics expert that major population's responses have neither a positive response nor a negative response which is (3.5). The researcher supposed that the acceptable level of the population' awareness is 21 which is counted upon the Likert-like scale of the questionnaire-3 (See Appendix A) as follows:

3.5 * (no. of question' items for each question)

3.5 *6 (See section 6.5.3).

The hypotheses used 21 as an acceptable value for the population's awareness.

The hypotheses are as follows.

Hypothesis 1:

H6.1: The respondents' awareness of secure email is different from the acceptable level of awareness (21) when they access their email for general purpose.

Hypothesis 2:

H6.2: The respondents' awareness of secure email is different from the acceptable level of awareness (21) when they access their email for family and friends' purposes.

Hypothesis 3:

H6.3: The respondents' awareness of secure email is different from the acceptable level of awareness (21) when they access their email for institution/organization purposes.

Hypothesis 4:

H6.4: Students' are aware of the importance of the security settings in order for the email to be secure.

Hypothesis 5:

H6.5: There are differences in awareness of secure email between students in Bahrain and students in the UK.

Table 6.1:Research questions and hypotheses

Main research questions	Sub-RQs	Hypotheses no.	Type of data analysis
6.1	6.1.1	N/A	Descriptive See section (6.5.2)
	6.1.2	N/A	Descriptive See section (6.5.2)
	6.1.3	N/A	Descriptive See section (6.5.2)
	6.1.4	N/A	Descriptive See section (6.5.2)
	6.1.5	N/A	Descriptive See section (6.5.2)
	6.1.6	H6.1,H6.2,H6.3	One-sample t-test See section 6.5.3
	6.1.7	H6.4	One-sample t-test See section 6.5.3
	6.1.8	H6.5	Independent t-test See section 6.5.3

6.4 Data collection methods

In this study, a quantitative questionnaire-3 was administered to the students in universities in both the United Kingdom (UK) and in the Kingdom of Bahrain (BH), to ascertain students' awareness of secure email.

The researcher has applied the "mixed methods" for data collection and "triangulation" for the validity of the survey discussed in the Chapter 3.

6.4.1 Student survey

The student survey was necessary to reveal the current status of students' awareness of secure email and identify the importance of secure email in Bahrain and the UK. The researcher's aim was to obtain details of students' awareness of emails for further in-depth investigation later in this study.

Design of the questionnaire

There were fifteen questions altogether. The details of each question are given below (See Appendix A):

1. The first section of the questionnaire-3 aimed to arrive at an understanding of the demographic background of the students, with questions covering the following:

- name, gender, address, age, nationality, course, email address;
- Type of Webmail they access.
- Email applications they access.
- Which email they access most frequently

The second section listed different terms (features) relating to secure email, and asked respondents to choose the possible meanings of these terms. The students were then asked which of these features were provided by their most frequent email service.

Based on the above information the respondents were asked to provide their perception (using a Likert-like scale) of how secure they believe their most frequent email is.

2. The questions in the third section focused on measuring the participant's awareness of email in six different questions, using a Likert-like scale. Both questions 10 and 11 related to the student's awareness and their experience of signing and encryption. Questions 12, 13 and 14 specifically related to secure email awareness, and were intended to evaluate how aware the students are of security when they access their most frequently used email in general. The respondents were additionally specifically asked

about how aware students are of security when they email their family/friends and important members of an organization. The researcher listed some security awareness actions and asked the respondents to choose how often they use them.

3. Question 15 listed some email security actions and asked the respondents to provide their perception of how important these actions are.

6.4.2 Pilot testing

A questionnaire of 12 questions regarding secure email awareness was presented to 10 external referees, comprising postgraduate students and staff members from the Computer Science department at the University of Warwick. The referees were asked to read each question and to comment on questionnaire items in terms of wording and content, and to give their comments and suggestions for improving the scale.

6.4.3 Reliability

Pilot testing was conducted to test the reliability of questions 12, 13, 14 and 15. The reason behind this is that these questions have sub questions on a Likert-like scale and the researcher needed this test so as to ascertain the internal consistency of all these items.

The researcher compiled responses from the ten questionnaires to assess the reliability of the student feedback questionnaire.

The reliability confidence (Cronbach‘s Alpha) for questions 12, 13, 14 and 15 were calculated as 0.7, 0.8, 0.8, and 0.8 respectively, which indicated that the items form a scale that has reasonable internal consistency reliability.

6.4.4 Validity

As previously stated, the questionnaire was initially shown to staff and postgraduate

student members of the Intelligent and Adaptive Systems group at Warwick University, so as to determine their opinion of the test items, and to ensure the test questions reflected the content and security aspects of email.

6.4.5 Respondents

Upon validation, with some minor modifications and alterations, the questionnaires were distributed to 400 students in paper and online form, with 200 being from either Warwick University and Coventry University in UK and 200 from either University of Bahrain or the Arab Open University. The pilot respondents were discarded in the main study. The researcher received 139 students from Bahraini students and only 114 from UK students. Substantial data was received from Warwick University and University of Bahrain, whereas less data was received from Coventry University and the Arab Open University, but they are sufficient to analyze.

6.5 Data Analysis

6.5.1 Quantitative analysis

Quantitative data provided us with quantifiable results, which was analyzed using SPSS software. Before using SPSS, some of the data was downloaded from the Warwick University web server where the questionnaire was hosted online by developing e-form for the questionnaire and others were from the paper based questionnaire (See Appendix A). The next section will present an analysis of each questionnaire and the results obtained.

6.5.2 Demographics and background details

This section addresses research questions 5.1 and 5.2. Table 6.2 shows data collected on both the demographics and the background details of the respondents.

Table 6.2: Demographics and background details of the respondents

Student demographics and background	Email clients	Bahrainis students /139		UK Students/114	
		No.	%	No.	%
Type of web email the students often use	Gmail	26	18.7	37	33.6
	Hotmail	72	51.8	22	20
	Yahoo	9	6.5	7	6.4
	Gmail/Yahoo	4	.7	8	7.3
	Gmail/Hotmail	9	6.5	11	10
	Gmail/Hotmail/Yahoo	17	12.2	20	18.2
	Missing/none/other	1	.7	7	6.2
Type of applications email the students often use	Apple mail	14	10.1	12	10.6
	Microsoft outlook	64	46	41	36
	Apple/Outlook	8	5.8	10	8.8
	Thunderbird	N/A	N/A	7	6.1
	Thunderbird/Outlook	N/A	N/A	4	3.5
	None/web mail only	53	38.1	16	35.2
How the participants often access their email	More than 9 times/day	6	4.1	43	37.7
	5 to 8 times/day	12	8.3	28	24.6
	1 to 4 times/day	48	33.1	37	32.5
	A few times a week or less	73	50.3	5	4.4

A. Type of web email the students often use

As shown in the above table, the majority of Bahraini respondents (51.8%) use Hotmail as a frequent email, whereas only 18.7% and 6.5% use Gmail and Yahoo respectively. Others use a mixture of Gmail, Yahoo, and Hotmail. These results indicate that students in Bahrain have familiarity with Hotmail rather than Gmail, and other web mails.

On the other hand, it may be noted that Gmail is the most frequently used web email (33.6% of the total) in the UK, with Hotmail the second most frequent which indicate that Gmail is webmail that has familiarity among the students in the UK.

B. Type of application email the students often use

Table 6.2 reveals that the majority (46%) of respondents from the total of the Bahrainis students use Microsoft Outlook and (38.1% of the total) use webmail only. On the other hand, only 10.1% use Apple mail.

Likewise, the majority of UK respondents (36%) have also chosen Microsoft Outlook, as a frequent email application.

C. Information on how the participants often access their email

Table 6.2 above demonstrates how often the students access their frequent emails in Bahrain and the UK per day.

It may be seen that the majority of Bahraini respondents (50.3% of the total) access their email a few times a week. Only 4.1% access their email more than 9 times per day. On the other hand, the majority of respondents (37.7% of the total) of the UK students access their email more than 9 times per day. It may be concluded that the students at Warwick University mostly access their email using university email and in the average usage over a period of 9 hours daily, and this suggests that a similar figure may apply to other UK universities

This data set shows that the students in UK mostly use Outlook as a common email application and the students use it in order to access their university email in their education. In fact, the university email has been chosen to communicate with students in both countries. Nevertheless, the students rarely use UOB email.

D. Security perception of email in general and in particular from the students' perception

The aim of the second section of the questionnaire-3 was to answer the RQ 6.1.3 in order to find out the UK and Bahrain students' perceptions about secure email compared with their perceptions about emails in general, and their frequent email in particular (See Appendix A).

The descriptive analysis shows that the majority of the respondents in Bahrain and UK have the perception that email is secure when its attachment is scanned, whereas few of the respondents have chosen other options. It seems that the students in both countries do not have secure email knowledge (See Appendix G).

E. Information about secure email and information on how secure they think their email is

After the evaluation of the students in the previous section regarding their perceptions of secure email, they were evaluated in terms of how secure they feel their most frequently accessed email is.

Table 6.3: Students' perception of the security of their email

Country		Very secure	Secure	Neither secure nor insecure	Insecure	Very insecure
BAH	Frequency	13	69	40	12	4
	Percentage	9.4	50	29.0	8.7	2.9
UK	Frequency	5	49	30	27	2
	Percentage	4.4	43.4	26.5	23.9	1.8

The overall results of the UK and Bahraini students, as depicted in Table 6.4, shows that the majority of the respondents (50% of Bahraini students) (43.4% of the UK students) feel that their most frequently accessed email is secure.

This data concludes that the students in both countries have the impression that their email is secure only if the attachment is scanned from viruses and they are not aware about security techniques of email such as signing and encryption.

The following section will reveal the awareness of signing and encryption

Signing and Encryption

This section of the questionnaire-3, which answers research question 5 aims, to investigate how often the students are aware of signing and encryption.

Table 6.4: How much the students use signing and encryption

	Q 10 (a, b)	Always		Most of the time		Some times		Occasionally		Never		I don't understand	
		No	%	No	%	No	%	No	%	No	%	No	%
BAH	Send email that is signed	24	17.3	6	4.4	8	5.8	16	11.7	69	50.4	14	10.2
	Send email that is encrypted	11	7.9	6	4.3	4	2.9	18	12.9	82	59.0	18	12.9
UK	Send email that is signed	3	2.7	4	3.5	17	15.2	14	12.5	57	50.9	17	15.2
	Send email that is encrypted	4	4.4	5	4.4	18	15.8	13	11.5	56	49.6	16	14.2

As may be seen from the overall results of the UK and Bahraini students, shown in Table 6.4, the majority of respondents have never used the signing and encryption technique in their email. Table 6.5 shows the reasons for this.

As shown in Table 6.5, the majority of the students in Bahrain (68.4%) do not care enough to do signing and encryption, 44.9% are worried that the other recipients are not able to read the encryption. Similarly, the majority of UK students (69% of the total) have no wish to engage in signing and encryption.

Table 6.5: Reasons for avoiding the student signing and encryption

Q11	BAH						UK					
What are the reasons beyond that?	Signed email		Encrypted email		Signed/encrypted		Signed email		Encrypted email		Signed/encrypted	
	No	%	No	%	No	%	No	%	No	%	No	%
It is too hard to do	34	46.6	31	42.5	8	11	92	80.7	5	4.4	17	14.9
I am worried that the recipient won't be able to read	25	36.2	31	44.9	13	18.8	4	3.5	11	9.6	11	9.6
I don't care enough to	6	5.3	2	1.8	78	68.4	6	8.5	1	1.4	49	69
I don't know how to	1	0.9	5	4.4	34	29.8	4	5.6	4	5.6	12	16.9

6.5.3 Results of the hypotheses test

In order to answer research questions 6.1.6, 6.1.7 and 6.1.8, and to test the hypotheses H6.1 to 6.4, the researcher used a questionnaire to gauge the student views in relation to secure email awareness. These hypotheses were tested for both Bahrain and the UK, using a one sample t-test. This kind of test finds out whether the mean of the responses of the questions 12, 13, 14 and 15 of the questionnaire is different from the neutral level (assumed to be an acceptable level of awareness) defined as 21. The acceptable level is decided by the researcher, and is counted as a multiplication of 6 (for 6 items of each question) and the neutral scale value (3.5).

Table 6.6: t-test details of Students' awareness of secure email

	BAH			UK		
Email access purpose	**t-test**	**P-value**	**mean**	**t-test**	**P-value**	**mean**
General purpose	14.038	0.000	15.44	33.298	0.000	10.5
Families/friends	8.316	0.000	17.05	17.75	0.000	13.7
Important member	10.038	0.000	16.35	15.35	0.000	13.5
Powerful organization	0.961	0.338	20.62	1517	0.132	20.4

A. Students' awareness of secure email for general purpose

The students were asked to answer question 12 in the questionnaire-3 (See Appendix A), related to their awareness of secure email when they access their frequent email for general purpose.

We can conclude from Table 6.6 that hypothesis H6.1 (which stated that the respondents' awareness of secure email is different from the acceptable level of awareness for the population when they access email for general purpose) is accepted (P=<0.05) and the mean is less than the acceptable level of awareness for both BAH and UK (15.44,10.5 < 21). Therefore the respondents have less awareness.

B. Students' awareness of secure email when emailing their families/friends

Question 13 related to the students' awareness of secure email when they contact their families and friends. Data analysis of the t-test for this question is shown in Table 6.6.

This concludes hypothesis H6.2, (which stated that The respondents' awareness of secure email is different from the acceptable level of awareness when they access email for their families and friends) is accepted (P<0.05) and the mean are less than the

acceptable level of awareness for the population for both BAH and UK (17.75, 13.7 < 21).

C. Students' awareness of secure email when emailing an important member of an organization

Question 14 related to the students' awareness of secure email when emailing an important member in an institution or organization. Data analysis relating to the t-test of hypothesis 6.3 is shown in Table 6.6.

Table 6.6 concludes that hypothesis H6.3 (stating that The respondents' awareness of secure email is different from the acceptable level of awareness for the population when they access their email for institution/organization purposes) is accepted and the mean are less than the acceptable level of awareness for the population for both BAH and UK (16.35,13.5 < 21).

D. The importance of security actions of the email is not different from the neutral level

In order to test hypothesis H6.4 which stated that "Students are aware of the importance of the security settings for the email to be secure " the students were asked in question 15 about their opinions regarding the importance of modifying security settings on their email. The result of the t-test is shown in the Table 6.6.

It may be concluded that the hypothesis is rejected for Bahrain and the UK because p >0.05 and the importance of security settings means are not different from the acceptable level of awareness (20.7).

E. Differences between the students' awareness of secure email in Bahrain and the UK

In order to test hypothesis H6.5 which stated that there are differences in awareness of secure email between students in Bahrain and students in the UK, an independent

sample t-test was applied. The following result concludes that the hypothesis H6.5 is accepted (t-test=9.720, df=247, P=0.000= P<0.05).

6.5.4 Qualitative analysis

A. Interviews result

In order to answer as well as clarify our research questions, some interviews were conducted with students in Bahrain and the UK. This involved two students from the University of Warwick, two students from the University of Bahrain and one lecturer from Arab Open University.

A semi-structured interview was designed in order to answer the research questions (See Appendix B for the interviews template). The overall structure of the questions was as below:

1. Students' perceptions about secure email aspects.
2. How often they access their frequent emails.
3. How aware they are of secure email.
4. Their viewpoint about future plans for email security and why.

- The majority of the interviewees from both countries stated that they do not know the security aspect of emails.
- The frequent email of the students in Warwick University is the university email, Microsoft Outlook.
- The interviewees in Bahrain stated that they do not frequently use their university email in their learning.
- The interviewees in both countries stated that they do not know about signing and encryption techniques, and they do not want to use it in future, because signing and encryption takes time to learn and to apply.

B. Results of open-ended questions

Some participants commented on question 10 which is related to signing and encryption, that their frequent email was secure and that they did not need to go through a complicated procedure.

6.6 Discussion of the result

The aim of this investigation was to gauge the students' awareness of secure email in Bahrain and the UK. In doing so, the researcher has conducted a questionnaire which has been analyzed using descriptive and t-test analysis. The findings of this investigation, together with hypotheses testing, have enabled the researcher to succeed in this aim.

Furthermore, participants from both countries access their university's email, which indicates that they use email in education. In addition to this, the evaluation reveals that Bahraini students often access their frequent email a few times a week, but most UK participants access their frequent email more than 9 times per day.

The questionnaire data analysis revealed that the majority from both countries have the same perception of secure email, in that they believed there email is secure when their attachments are scanned. But they were not aware of signing or encryption. This is confirmed with their answers to question 10 of the questionnaire in that not all the participants use signing and encryption with their email. Some participants stated that it is hard to do, while others did not know how to do so. This suggests that the participants from both countries were not aware of secure email. (Ghafoor *et al*, 2009) confirmed that when they stated "In practice most of email users send Emails in clear, because they don't have sufficient knowledge to configure security parameters. So, attacker can easily read and modify email letters." They also pointed out "security must be configured by

end–users who do not possess sufficient knowledge and it becomes inconvenient for the end user". (Ghafoor et al 2009)

Qualitative evidence from students' comments further supported this result, which shows that the interviewees in both countries do not know how to be aware of secure email and they do not know about most of the up to date security aspects such as signing and encryption.

The findings of hypotheses testing shows that the sample mean of students' awareness of secure email in both countries is smaller than the acceptable value for general purpose access. Additionally, their awareness of secure email is also smaller than the acceptable value when considering emails between family/friends or with powerful organizations. This indicates a lack of awareness.

On the other hand, investigation into the importance of secure email indicates that there are no differences between the sample mean and the acceptable level, when considering fixing the security with the emails is important.

The researcher has also tested hypothesis 6.4, which indicates whether there are any differences between Bahrain and the UK regarding participants' awareness of secure email. An independent sample t-test resulted in the acceptance of the hypothesis. In other words, there are differences between both countries with respect to the participants' awareness of secure email. This result may due to the different educational style in both countries. To confirm these results, the researcher conducted an intervention with the students in Bahrain and the UK in order to track their usage of daily email, which will be discussed in next Chapter.

6.7 Chapter Summary

The aim of this evaluation was to find out whether the participants in Bahrain and the UK are aware of the importance of security within email. The findings of this

investigation, together with the hypotheses testing, have enabled the researcher to successfully achieve this aim.

The survey was able to demonstrate which email the students' most frequently access. In addition to this, it revealed the perception of the students towards secure email.

Furthermore, hypotheses testing showed that awareness of secure email on the part of the participants differed from the acceptable level.

Moreover, there are no differences between participants in terms of secure email awareness in Bahrain and the UK.

In the next Chapter, secure email usage and awareness will be critically examined by conducting an intervention with the students in Bahrain and the UK to find out a clear picture of secure email usage and awareness.

Chapter Seven: Secure email tracking

7.1 Introduction

In this Chapter, an intervention has been done in order to find out a clear picture of secure email usage by the participants, how they access their frequently accessed emails, what kind of security attacks (spam, hacker and phishing) they face in the learning because the students can face spam and fishing attacks when they access their webmail in the learning. Then, their reaction towards security attacks over a period of 24 hours will be investigated.

This intervention would support the questionnaire-3 conducted in the previous Chapter and confirm the findings presented in previous Chapter. The following sections explain the intervention in detail.

7.2 Aims of the this intervention

The aims of this secure email intervention are as follows:

1. To find out the frequencies of sent and received emails for academic and non-academic purposes during one day;
2. To find out whether there are differences between academic and non-academic emails in terms of frequency of emails attacks, and action taken against them;
3. To confirm the results of previous activities discussed in the previous Chapters;

7.3 Research questions

RQ 7.1: What is the frequency of emails access for academic and non-academic purposes?

RQ 7.1.1 What is the frequency of emails sent for academic and non-academic purposes?

RQ 7.1.2 What is the frequency of emails received for academic and non-academic purposes?

RQ 7.1.3 Are there any differences between the frequencies of academic and non-academic emails?

RQ 7.2: Are academic and non-academic emails different to each other with respect to email attacks?

RQ 7.2.1: Are there any differences in the frequencies of embedded links that originate in emails from academic and non-academic sources?

RQ 7.2.2: Are there any differences in the frequencies of spam emails that appear to be for academic and non-academic purposes?

RQ 7.2.3: Are there any differences in the number of phishing attacks that appear to be for academic and non-academic purposes?

RQ 7.3: Are there any differences in the rates of action taken against attacks in emails which appear to be for academic and other purposes?

RQ 7.3.1: Are there any differences in the rates of the 'Ignored' action taken towards attacking emails which appear to be for academic and other purposes?

RQ 7.3.2: Are there any differences in the rates of the ‘Read & deleted’ action taken towards attacking emails which appear to be for academic and other purposes?

RQ 7.3.3: Are there any differences in the rates of the ‘Read & stored’ action taken towards attacking emails which appear to be for academic and other purposes?

7.4 Hypotheses

H 7.4.1: Students access their email for non-academic purposes more frequently than for academic purposes.

H 7.4.2: Students receive more embedded links in emails that appear to be from non-academic sources than in emails that appear to be from academic sources.

H 7.4.3: Students receive more spam that appears to be from non-academic sources than from academic sources.

H 7.4.4: There are differences between the frequencies of received phishing emails which appear to be from academic and non-academic sources.

H 7.4.5: There are differences in the frequencies of ‘Ignore’ responses taken against email attacks that appear to be from academic and non-academic sources.

H 7.4.6: There are differences in the frequencies of ‘Read and delete’ responses taken against email attacks that appear to be from academic and non-academic sources.

H 7.4.7: There are differences in the frequencies of ‘Read and store’ responses taken against email attacks that appear to be from academic and non-academic sources.

Table 7.1 shows the research questions, hypotheses and their aims:

Table 7.1: Research questions and its hypotheses and their aims

Main research questions	Sub-RQs	Aims	Hypotheses no.	Type of data analysis
RQ 7.1	RQ 7.1.1	1	N/A	Descriptive
	RQ 7.1.2	2	N/A	Descriptive
	RQ 7.1.3	2	H 7.4.1	Independent sample t-test
RQ 7.2	RQ 7.2.1	3	H 7.4.2	Independent sample t-test
	RQ 7.2.2	3	H 7.4.3	Independent sample t-test
	RQ 7.2.3	3	H 7.4.4	Independent sample t-test
RQ 7.3	RQ 7.3.1	3	H 7.4.5	Independent sample t-test
	RQ 7.3.2	3	H 7.4.6	Independent sample t-test
	RQ 7.3.3	3	H 7.4.7	Independent sample t-test

7.5 Data collection methods

In this activity, an observation form was administered to the students in universities in both the United Kingdom (UK) and the Kingdom of Bahrain (BH) at the end of the semester, to record the email tracking of the students over a 24-hour period. An online form as shown in Figure 7.1 and paper-based forms as depicted in Figure 7.2, were used as observation forms. The universities were chosen for their convenience in terms of accessibility to the targeted students and the ease associated with administering the evaluation tools to them, based on the fact that the author serves as a faculty staff member at University of Bahrain and a doctoral student at Warwick University in UK.

In order to aid the observation experiment, an informal observation format was used, with the researcher observing each one of the students individually by Skype to communicate

with them for the purposes of ensuring that they complete the activity as requested or contact by emails.

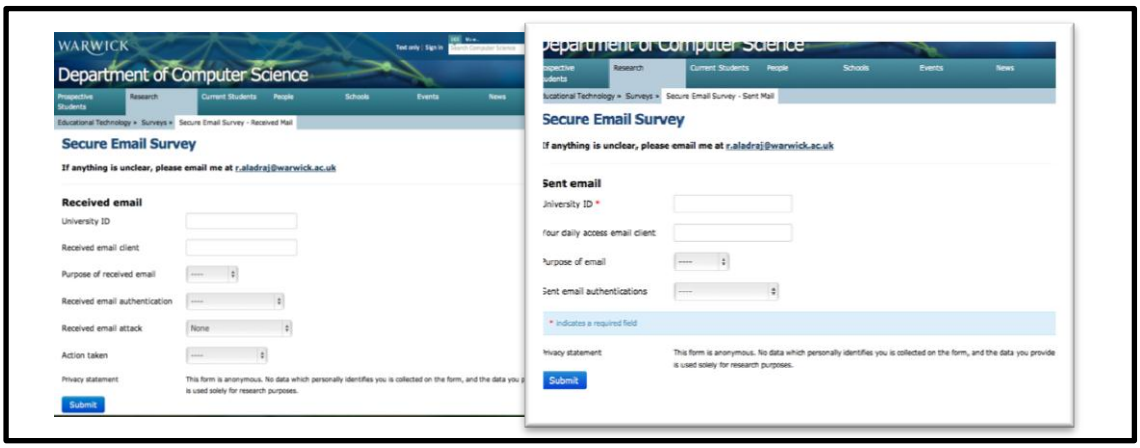


Figure 7.1: Screen shot of the online email tracking form

Email tracking form

The main aim of the tracking form was to track students' email by observing the following:

Sent email

- Time the email was sent.
- Purpose of the email (academic, social, or business);
- Whether the email was signed or encrypted.

Received email

- Time the email was received.
- Purpose of the email (academic, social, or business);
- Whether the email was signed or encrypted
- What attack (if any) was contained in the email (embedded link, spam, or phishing);

- For the same email, how the participants reacted (Read and stored, read and deleted, or ignored). These will be referred to as “action taken” in the rest of the document.

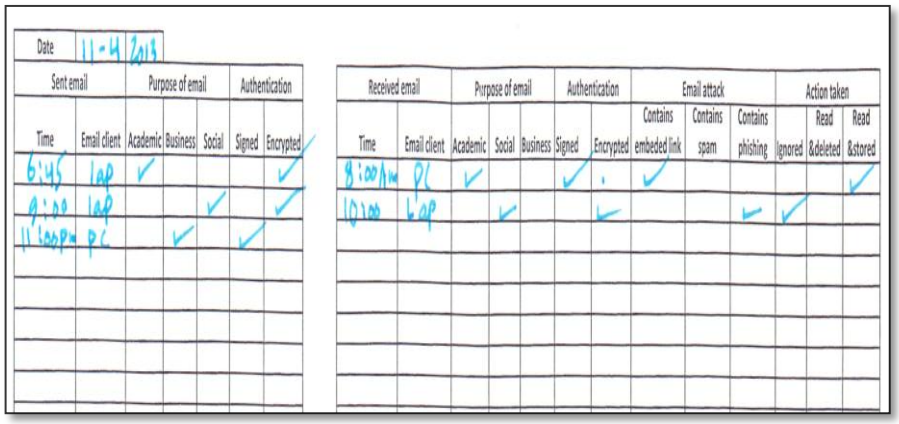


Figure 7.2: Email tracking observation form

Participants

In order to conduct the intervention, the researcher selected 75 students from the University of Bahrain and 40 students from UK, all are from either University of Bahrain or the Warwick University. However, 7 students from UOB were not able to complete the feedback, bringing the total number of students who completed the feedback to 68 and only 35 students from Warwick University completed the feedback. The resulting sample is therefore only representative of students from the University of Bahrain and Warwick University. It was not feasible in this particular study to identify a representative sample of students across all the universities in each country as the researcher had originally designed. Logistically it would be difficult to do a similar exercise in different universities in Bahrain and the UK due to the difficulty of the experiment.

7.6 Data analysis

In order to answer the research questions and test the hypotheses, quantitative and qualitative methods were utilized to analyze the data from Bahrain and the UK.

7.6.1 Quantitative method

Quantitative methods were utilized to perform descriptive and t-test analyses using SPSS software.

7.6.1.1 Descriptive analysis – sent and received email frequencies

In order to answer RQ7.1 and achieve aims 1 and 2, the researcher has drawn the following charts for the sent and received email within 24 hours for Bahrain and the UK participants as explained in the following sections.

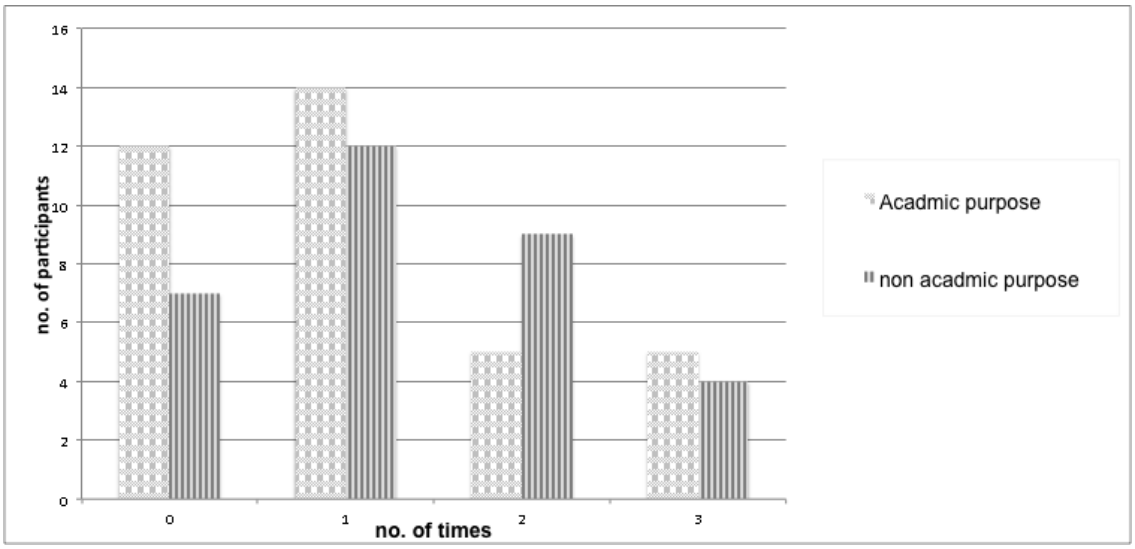


Figure 7.3: No. of emails sent /day by the participants in Bahrain

It is clearly shown from Figure 7.3 that the majority of the participants send emails once per day for both academic and non-academic purposes. However, an equal number of Bahrain participants send their emails two and three times a day for academic purpose.

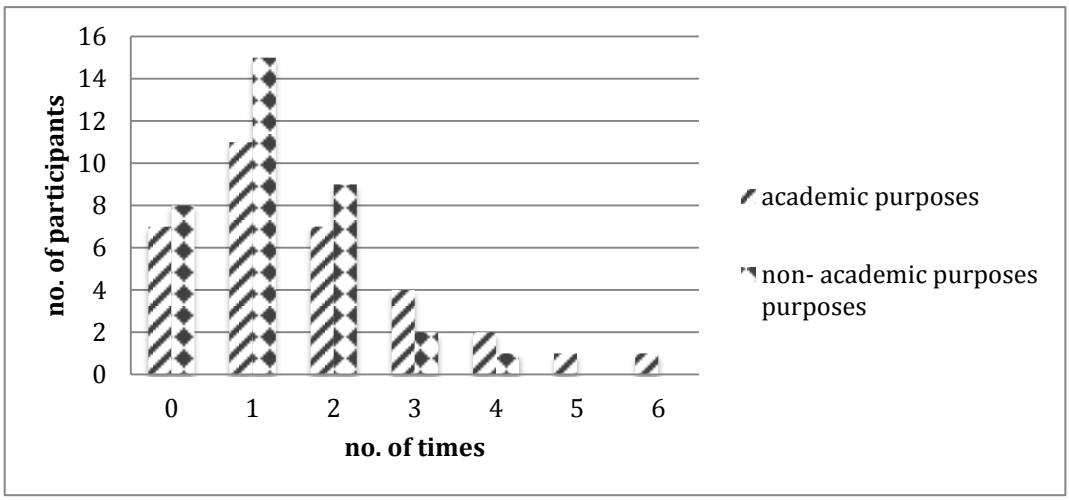


Figure 7.4: No. of emails received by the participants in Bahrain

It is clearly shown in Figure 7.4 that the majority of the total participants receive their email once per day for both academic and non-academic purposes. However, a minority of the total participants receive their emails four, five, and six times a day for non-academic purposes but still just once for academic purposes. A possible explanation is that some students prefer instead to communicate via IM tools such as Facebook or SMS rather than using email for their main means of communication.

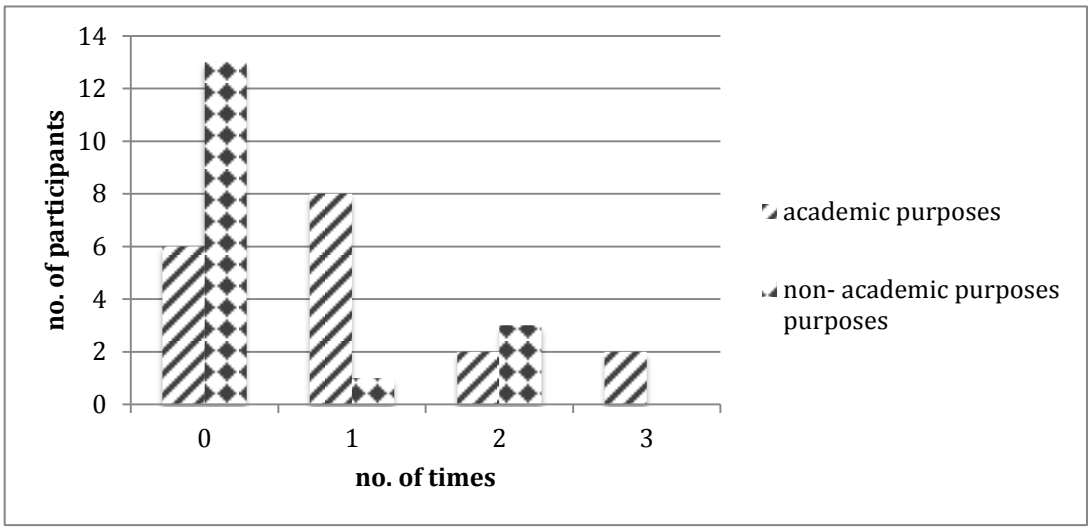


Figure 7.5: Send email frequency accessed by the participants in the UK

It is noticeably revealed in Figure 7.5 that for academic email, the majority of the total of participants receive emails once per day and the minority receive email two or three times a day. On the other hand for non-academic purposes, the majority (roughly 13 students) did not send any emails, whereas the minority (2 students) send emails for academic purpose once per day.

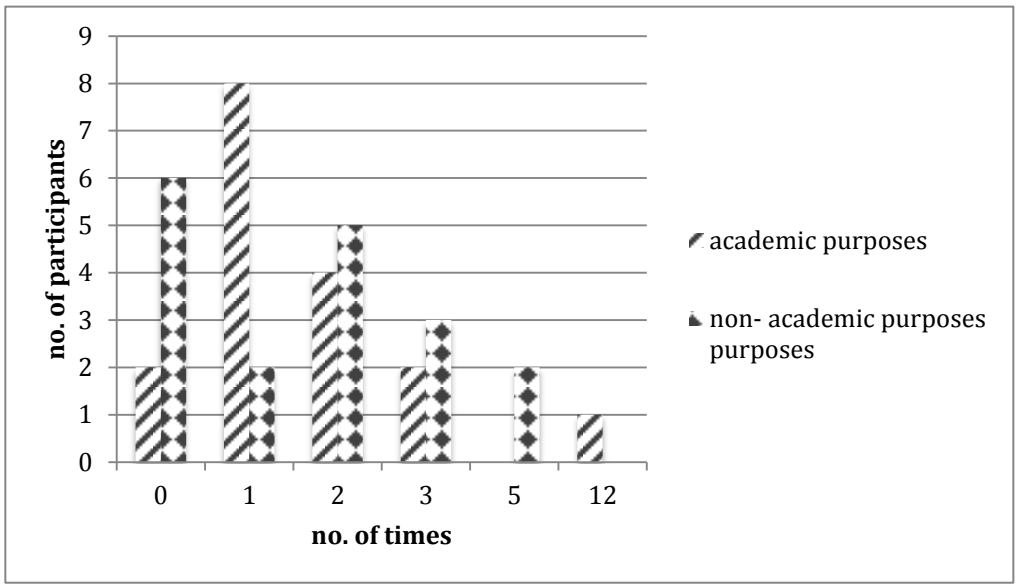


Figure 7.6: Rate of the Received email accessed by the participants in the UK

It is shown in Figure 7.6, for the academic purpose, the majority of the total of participants received emails one time per day and a minority received emails three and twelve times a day. On the other hand, for non-academic purpose, the majority of the total participants does not receive emails, and a minority of the participant receives emails five times a day.

7.6.1.2 Hypotheses testing

The received email usage frequency, attacks, and action taken were compared using an

independent sample t-test for both academic and non-academic purposes. The researcher's intention is to test the hypotheses listed above with respect to the purpose of the emails tracked.

The researcher used the t-test (independent sample t-test) (See Appendix E) in order to find out differences between the means of the samples of both sent and received emails for different purposes. The researcher used SPSS software to calculate the result of the t-test. The results of the hypotheses discussed above are shown in Table 7.2.

A. Hypothesis 7.4.1

As per Table 7.2, the first hypothesis (which indicates that there are differences between the frequencies of email accesses for academic and non-academic purposes) is rejected for both Bahrain and the UK (P>0.005). Thus, there are no differences between the frequencies of email access (for academic and non-academic purposes) for both countries.

Table 7.2: t-test of email usage rate of academic and non-academic

	t-test	Df	P
BAH	1.836	54.774	0.072
UK	0.597	33	0.555

B. Hypothesis 7.4.2

As shown in the Table 7.3 below, the t-test results shows that second hypothesis, (which states that there are differences between the frequencies of embedded links within emails that appear to be from academic and non-academic sources) is rejected for Bahrain and the UK (P>0.05).

Table 7.3: t-test of email attacks for academic and non- academic

	BAH		UK	
Email attacks	**T-test**	**P-value**	**T-test**	**P-value**
Embedded link	-0.293	0.770	-0.631	0.532
Spam attack	-2.781	42	-0.710	33
Fishing attack	-1.024	0.311	0.539	0.594

Therefore, there are no differences between the frequencies of embedded links associated with received email for academic and non-academic for both countries

C. Hypothesis 7.4.3:

The t-test results shows that the third hypothesis (which states that there are differences between the frequencies of received spam emails that appear to be from academic and those that appear to be from non-academic sources) is accepted for Bahrain as shown in Table 7.3 ($P<0.001$).

The differences show that the frequency of received spam emails from non-academic (0.4706) is greater than those that appear to be from academic (0.088). On the other hand, the hypothesis is rejected for the UK case ($P>0.05$).

D. Hypothesis 7.4.4:

The t-test results shows that fourth hypothesis (which states that there are differences between the frequencies of received phishing emails that appear to be from academic and those that appear to be from non-academic sources) for both the UK and Bahrain are rejected ($P>0.05$) as shown in Table 7.3.

E. Hypothesis 7.4.5:

T-test results shows that hypothesis 7.4.5 (which states that there are differences between the frequencies of "Ignore" responses taken against email attacks that appear to be from academic and non-academic sources) is accepted for Bahrain.

Table 7.4: t-test for action taken academic and non-academic emails

	BAH		UK	
Action against attacks	**T-test**	**P-value**	**T-test**	**P-value**
Ignore responses	-2.406	0.020	0.585	0.562
Read and delete	-0.432	0.667	0.562	0.578
Read and store'	-1.541	0.129	-1.060	0.297

Additionally, there was a higher mean rate of 'ignore' responses (0.382) for non-academic than for academic purposes (0.082). However, the hypothesis for the UK case is rejected as shown in the Table 7.4.

F. Hypothesis 7.4.6:

As shown in Table 7.4 hypothesis 7.4.6 (which states that there are differences between the frequencies of 'Read and delete' responses taken against email attacks which appear to be from academic sources compared with those from non-academic sources) is rejected for Bahrain and the UK.

G. Hypothesis 7.4.7

Table 7.4 shows that hypothesis 7.4.7 (which states there are differences between the frequencies of 'Read and store' responses taken against email attacks which appear to be from academic sources compared with non-academic sources) is rejected for Bahrain and the UK.

7.6.2 Qualitative analysis

Interviews

The researcher conducted interviews with two faculty members from the computer science department. The faculty members teach on a security module that teaches students about signing and encrypting emails. Additionally, the researcher interviewed two postgraduate students at Warwick University. The interviews were carried out in order to pinpoint and extract the specific difficulties and problems faced by the students in applying signing and encryption. The interviews also aimed to harness their views about the use of this technique as a teaching and learning resource.

The interviews asked the interviewees two questions:

1- Do you know what is "signing and encryption"

2- How often they apply them when they access their emails?

A. Academics' views

The responses of the two academics were as follows:

A1 and A2 exchange encrypted emails between themselves and some other faculty members and they sent a few encrypted emails during the weekday because they do not know if the recipient would decrypt, or whether they know how to do so.

B. Student's views

The responses of the PhD students were as follows:

1- P1 commented "we think carefully about encrypting but we cannot do so because we do not know if the recipients can decrypt or understand the signature.

2- P2 pointed out "we do not know what "signing and encryption" means, and we think it would be hard for them to learn it and indeed they understood the "signed" check box as a graphical signature that can be inserted from the email menus."

7.7 Discussion of the result

The aim of this intervention is to reveal a clear representation of secure email usage over a one day period for both academic and non-academic purposes (such as social and business) used by participants (students and staff) in Bahrain and the UK.

It is concluded from the descriptive analysis that the frequency the participants accessed their email differed in Bahrain and the UK. The intervention showed that the majority of the total participants in Bahrain frequently accessed (mostly once per day) their email for academic and non-academic purposes, whereas in the UK it was noticed that the participants sent and received academic emails more than non-academic emails (mostly once per day). These results conclude that the students in the UK access their emails more frequently for academic purposes than Bahraini students. A possible reason behind this may be University of Warwick provides students with the Outlook email platform and it is simple for them to access. This reason is not yet established and will be considered in the next experiment.

In order to test the hypotheses and ascertain whether the sample mean of the received email attacks for academic and non-academic purposes are different, the participants in Bahrain and the UK were required to track their email and notice if their email included any embedded links, spam or phishing. It was noted from the t-test that there was no difference between the number of attacks in Bahrain and the number of attacks in the UK. In addition to that, most of the participants receiving emails in Bahrain had more spam attacks when opening non-academic emails.

With regard to the action taken against the attacks, the hypotheses results concluded that there were no differences between the actions taken against academic emails, and those taken against non-academic emails, for either Bahraini or UK respondents.

However, in Bahrain there was a difference between the number of "ignore" actions taken against attacks sent to academic addresses and those taken against emails sent to non-academic addresses attacks in Bahrain. In other words, the students in Bahrain do not have sufficient awareness of email attacks. The t-test data revealed that they ignore attacks against non-academic more than attacks against academic emails.

It was noted that there are also issues with signing and encryption security techniques. The majority of participants did not use signing or encryption, only a minority said that they signed their emails. Interviews analysis revealed that these students understood these terms as a graphical signature.

Limitation of the intervention

1- Due to time constraints, students' participation in the UK occurred when exams were conducted, and the response rate was therefore not as high as would be desirable.

2- As discussed in the previous section, most of the students did not understand terms such as "signing" or "encryption", which led them to leave most of the checkboxes blank; the researcher discarded these.

3- It was not possible to follow all the participants and a large survey might wish to look at further opportunities for a more comprehensive study.

7.9 Chapter summary

This intervention was aimed at providing a clear picture of secure email usage and awareness, how the students access their frequent emails, what kind of security attacks they faced, and their feedback regarding the security attacks within a 24 hour period.

This intervention concludes from the t-test that the hypotheses are accepted (except hypotheses 7.4.3 and 7.4.5) for the Bahrain cases, which indicates that there are

differences between academic and non-academic emails with respect to spam attacks and ‘ignore’ actions taken against email attacks in Bahrain.

Therefore, following on the success of the experiment to clarify the participants’ perception in UOB towards their email, the focus will now shift to how to educate the students at the University of Bahrain about securing email, thereby increasing the frequency of secure email usage in their learning. The next Chapter will explain the intervention created to overcome that problem.

Chapter Eight: Validation of the Research Framework

8.1 Introduction

In the first stage of the research, after the primary research, a quasi-experiment which was described in Chapter 4 was conducted to evaluate the security, safety and privacy of selected OCG tools used during learning activities. This focused on the impact of their usage on OCG trust and on the motivation of the students. Skype, Wikis, Facebook, and Gmail (SWFG) were the OCG tools used in order to apply the quasi-experiment. The main results that related to emails are as follows:

- Secure Gmail has a significant but negative relationship with Gmail usage.
- Secure Gmail is significantly but negatively related to Gmail trust.

In the second stage (Chapter 5), an evaluation was carried out on secure email awareness. In the third stage (Chapter 6) an intervention for tracking students' email was conducted in order to find out how the students accessed their emails for their academic purpose in one day. The intervention established that there are no differences between the number of times email is accessed for academic and non-academic purposes. Furthermore, the students in the UK and in Bahrain did not know many of the security aspects of email, especially signing and encryption, how they work or what their benefits are.

The aim of this "one shot" case study is to validate the contextual framework which has been resulted from the previous intervention, as shown in Figure 8.1, and to answer the research questions and test the hypotheses listed below.

(Yin.R,2004) cited in (He et al, 2014) claimed that "case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially

when the boundaries between phenomenon and context are not clearly evident. In terms of the research strategy, case study comprises an all-encompassing method-covering the logic of design, data collection techniques, and specific approaches to data analysis. It is a comprehensive and integrated research approach."

The researcher followed the pre-experimental design according to the post-test one-shot case study type. The available sample was used since it serves the purpose of assessing the effectiveness of the experiment (AlKhalili, 2014).

8.2 Specific Objectives

The objectives of the case study were:

1. to validate the effectiveness of the proposed framework to enhance email usage in learning;

2. to engage students with the security aspects associated with email;

3. to determine the student's perception of secure email in terms of trust, ease of use, and usefulness;

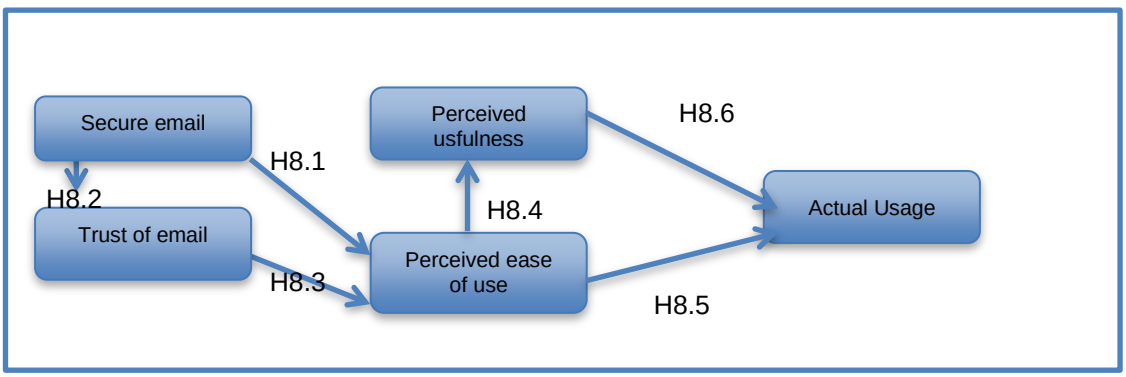


Figure 8.1: The research framework (Email acceptance model) derived from the Technology Acceptance Model (Hubona, 2003)

8.3 Research questions

In conducting this case study the researcher has developed five research questions as follows:

RQ 8.3.1: Does secure email positively relate to perceived trust of email?

RQ 8.3.2: Does secure email positively relate to perceived ease of use of email?

RQ 8.3.3: Does trusted email positively relate to perceived ease of use of email?

RQ 8.3.4: Does perceived ease of use positively relate to perceived usefulness of email?

RQ 8.3.5: Does perceived ease of use positively relate to actual usage of email?

RQ 8.3.6: Does perceived usefulness positively relate to actual usage of email?

RQ 8.3.7: Are the students' perceptions of webmail independent of webmail provider?

8.4 Hypotheses Testing

The following are the hypotheses that are derived based on the previous research questions:

H8.1: Secure email is related to perceived trust of email.

H8.2: Secure email is related to perceived ease of use of email.

H8.3: Trusted email is related to perceived ease of use of the email.

H8.4: Perceived ease of use is related to perceived usefulness of email.

H8.5: Perceived ease of use is related to actual usage of email.

H8.6: Perceived usefulness is related to actual usage of email.

H8.7: Students' perception of webmail is dependent on webmail type.

8.5 Experiment details

For the purpose of the research, the first, and perhaps most important step, is to set up email security practices for the participants. The researcher developed a training prototype which was divided into two main programs.

The experiment took three weeks for three different classes of students of different levels.

8.5.1 Prototype stages

Stage1: Grouping the students

- The participants in each class were distributed into groups according to the project group that had been assigned by their teacher at the beginning of the term.
- The participants were asked about their frequent webmail usage.

Stage 2: Training program

- Security settings guidelines which will be discussed in the next section were distributed among the students.
- The participants were allowed to follow the guidelines for the security setting for a single time with the help of the researcher.
- The participants were allowed to communicate with each other by emails in the class and at home.
- Their teacher changed her office hours from face to face to email communication.
- The teachers distributed their assignments by email.

Stage 3: Follow up

In order to allow the researcher to follow up the participants, the following procedure was implemented:

- The researcher and the course teacher received copies of participants emails as "CC".
- Follow up sheets were distributed among the participants as shown in Figure 8.1 in order to follow up the participants during the experiment. The sheet asked the students to fill in the following details:

- Time of receiving/sending email
- Purpose of the emails
- Webmail type
- Type of email attacks
- Type of action taken

- Additionally, the researcher followed them up by using a phone chat application (whatsapp).

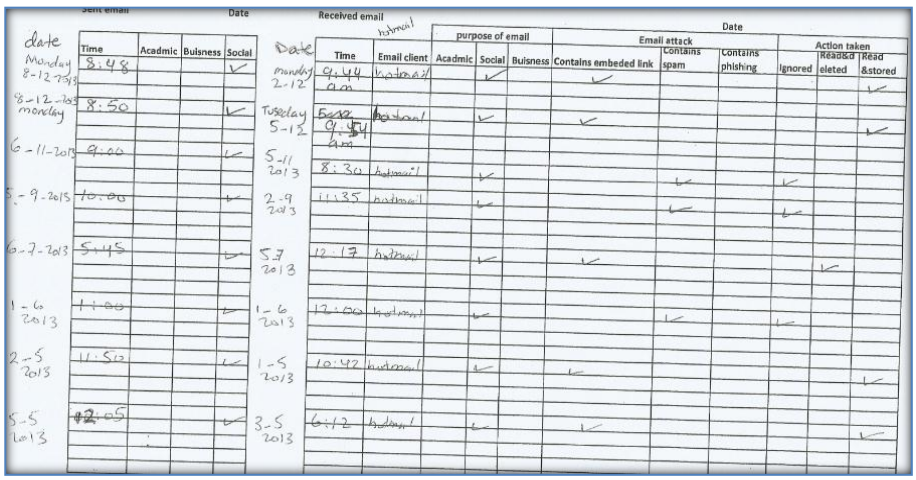


Figure 8.2: Follow up sheet

8.5.2 Prototype design

The training program of the prototype included both pedagogical and technical guidelines. Sample technical guidelines for the security settings can be found in Appendix C.

A. "How to secure Gmail and Hotmail" guidelines were distributed amongst the participants. The researcher chose the following most important, common and straightforward security processes.

B. Two-step verification

This step helps protect the email account by making it more difficult for a hacker to sign

in by prompting the user to enter a security code to sign in. Then a new security code is sent to the user's phone or alternative email address. This step uses two methods of verifying the user's identity when they sign in to their email account: password and an extra security code.

C. Enabling HTTPS security

HTTPS encrypts the data sent and received with SSL, while HTTP sends it all as plain text. The participants were asked to always write "HTTPS" in the URL address in order to secure their data. This process is explained in the guidelines (See Appendix C).

D. Checking account activity

The command **"Last account activity"** can check for suspicious logins and password changes. For example, in Gmail this command appears below the inbox.

Participants were particularly instructed how to check "Junk emails" for deleting junk mails and stopping spam.

Participants were also educated on reviewing tagged or filtered messages to identify ones that have been incorrectly labeled:

E. Filtering

The researcher trained the users to configure filtering features such as creating lists of safe senders and lists of senders to block.

The following are the managerial guidelines for pedagogical purposes which were given to the students in order to know how to manage and get the benefit of email usage in the learning.

F. Creating labels

This step is to create folders in which to organize incoming and outgoing emails and

course materials.

G. Demonstrating email tasks

This step allowed the user to perform the tasks related to an email message the user received.

H. Starring items

Users can star the emails messages to easily mark certain messages as important or to indicate which ones need to be replied to later.

8.6 Methodology

Throughout this study, the researcher was aware of the need to gather only sufficient, legal and reliable data that is relevant to the work, and not to be hampered with unnecessary data.

There were two methods for collecting the data, quantitative and qualitative methods.

8.6.1 Quantitative method

Questionnaire survey

The researcher developed questionnaire-4 to be distributed amongst the participants at the end of the experiment to collect the participants' perceptions.

A. Construct of the instrument

There were 32 questions altogether in the questionnaire-4, grouped into seven sections. The details of each question are described below (See Appendix A for a copy of the full questionnaire).

-The first section of the questionnaire-4 aimed to discover the demographic background of the students, with questions covering age, year of study, course, etc.

-The second section obtained information regarding the types of webmail the students

used during the experiment.

-The eight sub-questions in the third section focused on measuring each participant's perception of how secure their frequent emails were during the experiment. The sub-questions used a five-point Likert scale and were derived from the email security settings, which were given to the students during the experiment so that they could apply them to their emails.

The question in section 4 measured the frequency of email usage by the students during the experiment using (never, rarely, occasionally, often) measurements.

-The question in section 5 measured how much the participants trusted the emails they received after setting the security during the experiment. The questions were derived from McKnight et al (2002).

-Section 6 measured perceived usefulness of email during the experiment using a five-point Likert scale of (strongly agree, agree, undecided, disagree, and strongly disagree). This section includes six questions which were adapted from Hubona (2003).

-Section 7 similarly measured perceived ease of use during the experiment.

B. Validation

Construct validity

The researcher has conducted the construct validity of the instrument to ensure that each item measures what it is intended to measure. The aspects of the questionnaire such as trust, perceived ease of use, perceived usefulness and actual usage were taken from some of the journals and articles cited in Chapter 2. Security guidelines were derived from the "security settings" of Gmail and Hotmail.

For this purpose, the researcher made a comprehensive review of previous attempts to measure the variables that were investigated in the present study.

Face validity

The questionnaires were presented to a panel of judges consisting of 10 faculty members from the IS Department in the IT College at the University of Bahrain, and a statistician who works as a vice director at the scientific publishing center. The referees were asked to read each question and to comment on the questionnaire items in terms of wording and content, and to give their comments and suggestions for improving the scale.

Pilot testing

Pilot testing was conducted to test the validity and the reliability of the questions used in the questionnaire as follows:

Reliability

The researcher compiled responses from twelve students to assess the reliability of the student feedback questionnaire. The researcher conducted preliminary testing of the questionnaire among twenty-five students selected at random. The researcher was able to collect all twenty-five responses for the purpose of this pilot study.

Table 8.1 Reliability Statistics for Pilot study

No. of question	Factor	Cronbach's Alpha	Number of Items
3	Security	0.649	8
5	Trust	0.806	8
6	Usefulness	0.801	6
7	Ease of use	0.775	6

The questionnaires were tested for reliability to ascertain the internal consistency of questions 3, 5, 6 and 7. Table 8.1 shows the reliability confidence (Cronbach's Alpha) for questions 3, 5, 6 and 7 which are all >0.7 (showing

reasonable internal consistency) except the Security factor (0.649) which is acceptable. This was deemed to be acceptable, and was not changed because in order to identify the participants' perceptions of the practice tasks, the security items in the questionnaire must be based on the security settings that are available within the webmail services.

C. The Sample

After validation, with some minor adaptations and amendments, the questionnaires were distributed to 100 students of the available classes. The pilot respondents were discarded in the main study. The researcher received 91 responses only. The sample was chosen randomly from students in the IS Department in the IT College at the University of Bahrain.

8.6.2 Data analysis

Quantitative data provided us with quantifiable results, and data collected through tools such as the questionnaire were analyzed using SPSS software. Descriptive as well as analytical statistics were used. Correlation coefficients, means and standard deviations were obtained.

The multivariate analysis was used for testing the seventh hypothesis (H8.7). The next section presents the results of these analyses.

A. Descriptive analysis

The following are the discussions of each point using descriptive analysis.

Email clients used during the experiment

It is evident in Table 8.2 that the most frequently used email by the participants was Hotmail (40.7%). The second was Gmail (34.1%). However, Yahoo is the least used.

Table 8.2: Frequency distribution of web mails used during the experiment

	Frequency	Percent	Valid Percent	Cumulative Percent
Often	8	8.8	8.8	8.8
Occasionally	42	46.2	46.2	54.9
Rarely	28	30.8	30.8	85.7
Never	13	14.3	14.3	100.0
Total	91	100.0	100.0	

Actual email usage by the participants during the experiment

Table 8.3 shows that 46.2% of the participants indicated that they have used email for learning occasionally (46.2%), and about one third (30.8%) rarely. However, 8.8% of the participants used email for learning regularly.

Table 8.3: Actual email usage during the experiment

Webmail's type	Frequency	Percent	Valid Percent	Cumulative Percent
Yahoo	9	9.9	9.9	9.9
Gmail	31	34.1	34.1	44.0
Hotmail	37	40.7	40.7	84.6
Gmail + Hotmail	14	15.4	15.4	100.0
Total	91	100.0	100.0	

B. Hypotheses testing

In order to answer the above research questions and to test hypotheses 8.1 to 8.5, the researcher used a questionnaire to gauge the student perceptions in relation to secure email usage.

Table 8.4. Pearson Correlation Coefficients between the targeted Variables

		Secure email	trust	Perceived usefulness	Perceived ease of use	Actual usage
Secure email	Pearson Correlation	1	.575**	.420**	.502**	-.150
	Sig. (2-tailed)		.000	.000	.000	.156
	N	91	91	91	91	91
Trust	Pearson Correlation		1	.519**	.614**	-.183
	Sig. (2-tailed)			.000	.000	.083
	N		91	91	91	91
Perceived usefulness	Pearson Correlation			1	.452**	-.189
	Sig. (2-tailed)				.000	.073
	N			91	91	91
Perceived ease of use	Pearson Correlation				1	-.215*
	Sig. (2-tailed)				.000	.040
	N				91	91
Actual usage	Pearson Correlation					1
	Sig. (2-tailed)					
	N					91

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

The researcher chose Pearson correlation to test the hypotheses in section 8.5 to find out whether hypotheses 8.1 to 8.5 are accepted or rejected. Pearson coefficient was chosen as it is the most common and usable proposition for normal distribution.

Table 8.4 shows that the correlation between secure email and perceived ease of use and trust of emails were found to be 0.502 and 0.575 respectively; which are highly significant (α =0.01). Thus, the first and second hypotheses (8.1 and 8.2) of the study are accepted, and we conclude that secure email and both 'perceived ease of use' and 'trust' are positively correlated.

Furthermore, the correlation between trusted emails and perceived ease of use was found to be 0.614 which was found to be significant (α=0.01). Thus the third hypothesis (8.3) of the study is accepted and we conclude that trusted email is positively related to perceived ease of use of the email.

In relation to hypothesis 8.4, which stated that perceived ease of use is related to perceived usefulness of the email, as shown in the Table 8.3, it is evident that the correlation between them (0.452) is significant (α=0.01). Thus, hypothesis 8.5 is accepted.

Table 8.4 shows that the correlation between ease of use and actual use was found to be -0.215 which was found to be significant (α=0.05). It is evident that hypothesis 8.5 is accepted but with negative correlation. This means that perceived ease of use is *negatively* related to actual usage of email.

However, it is evident from Table 8.4 that the correlation between perceived usefulness and actual usage found to be -0.189, which was found not to be significant (α=0.01 and α=0.05). We can conclude that hypothesis 8.6 is rejected. Thus, perceived usefulness is

not related to actual usage of email.

Results Pertaining to Students' Perception of Webmail

In order to test the hypothesis 8.7, which states that students' perception of webmail is dependent on webmail type, the researcher has calculated the multivariate analysis of variance (MANOVA) and univariant analysis tests by SPSS software (See Appendix E). Table 8.5 shows that the mean scores given to each of the four types of webmail on the four dimensions of students' perception of webmail (secure email, trust of email, perceived usefulness, and ease of use) are nearly the same, fluctuating around the same values. The multivariate analysis of variance (MANOVA) results (See Table 8.6) show non-statistically significant differences between the four types of webmail (Wilks' Lambda=0.873, F= 0.976, Sig. level=0.473). The results of the one way ANOVA tests (See Table 8.7) showed non-statistically significant differences of students' perception of webmail on each of the four dimensions of this perception.

8.6.3 Qualitative method

The qualitative data of this study includes non-numerical data obtained from interviews conducted with the IS department's teachers. The researcher conducted unstructured interviews before and after the case study with the teachers and the participants. These interviews are useful for finding out the participants' opinions regarding email usage in learning which cannot be measured by questionnaires only.

Burgess (1982) defined interviews as the opportunity of the researcher to probe deeply to uncover clues, open new dimensions of a problem and secure vivid, accurate and inclusive accounts that are based on personal experience.

However, Silverman (1993), Zikmund (1997) and Bell (1999) point to criticism of interviews in that they require a personal sensitivity, adaptability and a need to stay within the bounds of the designed protocol. In addition, interviews are very time-consuming and they are resource intensive.

A. Pre-case study interviews

Aims of the interview

The researcher conducted interviews with a sample of lecturers and students from the IS department. The aim of these interviews was to obtain the specific profile of the emails used in the learning as well as the difficulties faced by the lecturers. Additionally, the interviews aimed to get their views on the use of email as a teaching and learning assistance teaching tool.

Design of the interview

Unstructured interviews were used to determine the current difficulties and problems faced by the IS lecturers at UOB. The study further looked into the identification of suitable areas for using advanced multimedia. Interviews were conducted with three IS teachers and five students. The interview questions consisted of the following four areas related to the subject matter being investigated.

1. Web mails usage in learning.
2. UOB email usage in learning.
3. The problems faced in using emails in learning.
4. What solutions may solve these problems?

The teachers' responses

Email usage

Most lecturers commented that they do not use UOB email in the learning and this is due to lack of encouragement by UOB. On the other hand, most of the students have their own webmail but they do not use them in the learning due to the teachers' discouragement.

The problems faced in using emails in the learning

Most of the lectures noted that one of the problems faced by the students was that they do not trust using email as a communication tool, especially for documents and assignments. This is due to the lack of security.

Possible solutions

The teachers suggested training students on how to secure the webmails and encouraging them to use them as a teaching tool particularly when they work in the course project groups.

The participants' responses

The students agreed with what their teachers had said in that they do not use UOB emails and they rarely use the webmail in the learning due to the lack of trust in emails. Furthermore they pointed out that their teachers do not give them the opportunity to use it as a teaching tool.

B. Post-case study interviews:

Aims of the interview

The aim of these interviews was to obtain the specific view of the lecturers and the students about using emails in the learning, as well as to discover the difficulties faced by the lecturers when using email during the experiment.

The interview questions consisted of two areas relating to participants' perception.

1. The problems faced in using emails in the learning
2. The participants' feelings during and after the experiment.

The teachers' responses

The researcher interviewed the course lecturer as well as some of the students at the end of the experiment.

The lecturer L1 commented that she was very pleased during the experiment. She commented "As a teacher, email usage in the learning facilitates the communication with the students and lets me exchange the assignments and documents with the students without the need to restrict on the office timing". In addition to that, she pointed out that "the guidelines of how to secure the emails was very easy and the students can set them up only for one time. I think I will use emails in my teaching…"

The students' perceptions

The researcher interviewed 6 students from different classes at the end of the experiment. Most of them felt pleased, and they felt motivated to use the emails in the learning. SS1 stated that "email usage in the learning is very useful if we get support from our teacher". Furthermore SS2 pointed out "I felt confident when I was using the email, particularly after the security settings."

Open observation

Participation:

The researcher observed that the participants were confused about how to fix the security settings. However, when the researcher put a mentor for each group to fix the security settings for their email they became active and they sent emails between each other and with their teacher.

On the other hand, there were some participants in the class who did not access their email during the case study.

Security settings fixing:

The researcher has observed difficulties in setting up the following practices:

1- Two-step verification;

2- Manage to filter the email

3- Manage to clean their email from spam and phishing

8.7 Conclusion and discussions

In this Chapter, the researcher conducted a one-shot case study as identified earlier in the Chapter to validate the contextual framework, which has resulted from the previous intervention as shown in Figure 8.1 and to answer the research questions and test the hypotheses listed above. The following conclusions were driven from the hypotheses testing:

H8.1 and H8.2: Perceived ease of use and trust are both positively correlated with secure email.

H8.3: Trusted email is positively related to perceived ease of use of the email.

H8.4: Perceived ease of use is positively related to perceived usefulness of the email.

H8.5: Perceived ease of use is negatively related to actual usage of email.

H8.6: Perceived usefulness is not related to actual usage of email.

Thus, the framework depicted in Figure 8.1 has been validated for only hypotheses 8.1 to 8.4. In other words, the researcher can confirm that secure email and trusted emails lead to ease of use, which in turn lead to usefulness. Moreover, ease of use relates to usefulness which is already validated by (Hubona & Burton-Jones, 2003). However, the

result of this case study clashes with (Hubona & Burton-Jones, 2003) because H8.5 was accepted but with negative correlation. In other words ease of use and usefulness have a significant relationship but it is negative which cannot validate the frame work. Additionally, H8.6 is rejected. Thus, there is no relationship between perceived usefulness and actual usage of email. Therefore, we can conclude that the research frame work is not validated.

Moreover, descriptive analysis shows that many of the participants indicated that they have used email for learning occasionally, and about one third (30.8%) rarely. However, 8.8% of the participants used email for learning regularly. Additionally, the email service used most frequently by the participants was Hotmail (40.7%).

Quantitative and qualitative analysis indicated that UOB participants were not aware of how to use secure emails for learning purposes. This was clear from the interviews and observations which support the hypotheses analysis. The following limitations prevent validation of the framework:

1- Lack of the students' and teachers' knowledge of security settings in email;
2- The teachers do not motivate their students to use the email in the learning;
3- UOB administrators do not encourage the students and teachers to use UOB university email;
4- The researcher spent time to explain to the students how to secure emails. This let the students to think that these were lectures and they felt bored;
5- The researcher had difficulties finding a sample of students that were willing to adjust their security settings;
6- Some of the students were not cooperative with the researcher in that they did not use the emails in the learning during the case study.

The researcher will conclude the study in the next Chapter with discussion, recommendations and conclusions sections.

Chapter Nine: Discussions, Recommendations and Conclusions

9.1. Introduction

This study aimed at conducting research in order to produce an innovative design model for the secure email usage to support the learning process focusing on Bahrain. The specific objectives of this study were to determine the effectiveness of the proposed design model to enhance learning, and to identify where the proposed design model could be adapted to enhance teaching in other countries and subjects.

In the first stage, initial study (described in Chapter 4) was carried out to identify the primary issues and problems faced by both students and teachers while applying OCG tools in the learning process. The primary research was conducted with students using a quantitative questionnaire, and with teachers using qualitative interviews in Bahrain. This research had the broader objective of examining the experience of OCG tools usage by both the students and faculties.

In the second stage (Chapter 5), a quasi-experiment was carried out with the students at UOB. The aim of this experiment was to identify the perception of the students towards security, privacy, safety, usage of SWFG during the learning process. This quasi-experiment mainly produced quantitative data, but to a lesser extent also collected qualitative interviews, log files and observation data

In the third stage (Chapter 6), email examined in the previous stage was further evaluated with respect to security using student feedback from both qualitative and quantitative methods in the form of a questionnaire and informal observation and interviews. This was because the experiment conducted by the researcher in the previous

stage indicated that email does not have a high level of security. Hence, the researcher conducted a survey in order to reveal the students' awareness towards the secure email.

In the fourth stage of this study (Chapter 7), an intervention was carried out in order to monitor a clear picture of secure email usage by the participants during 24 hours. This activity confirmed the previous stage in that it demonstrated the participants' reaction and awareness of secure email.

Finally, in the fifth stage (Chapter 8), the research framework was validated using a one-shot case study to test the security dimensions: namely, secure email, trusted email, perceived usefulness, and perceived ease of use. The following sections present the discussions of the main findings of this study.

9.2 Discussion of the finding from the initial primary research

The results from the primary research stage revealed that most of the OCG tools (such as IM, Social media, Forums, and email) are familiar and effective tools to the students. Moreover, the majority of respondents agree that social media has a good authorization whereas YouTube and wikis have poor authorization. With respect to the security solution and technologies, most of the respondents use antivirus as a security solution and password as security technologies.

Regarding the privacy, most of the respondents prefer the data of their assignments, courses, collaborative, and their personal data to be private and confidential to the administrator only.

From these initial results, the researcher proposed that for teaching-learning to be purposeful and effective for the benefit of the students, it needed to be based on IM, Social media, Forums, and email, as they are effective and secure. Moreover, the teachers and the students must be introduced with the new and up-to-date security

technologies in that they can make such tools more secure. Simultaneously, the students and their teachers must be introduced to OCG tools that make the data more private such as email and Facebook.

OCG tools provide a technology-rich learning environment, and are recognized as being more beneficial to students in terms of sense empowerment (Trinidad, 2003), (Khine & Fisher, 2003), (Bransford et al1999), (Albon and Trinidad, 2001) because technologies such as these allow the educator to identify an educational society that exceeds the classrooms but is not restricted by old-style class timeframe.

The results of the students questionnaires applied in the primary research supports (Danyaro *et al*, 2010) and (Wei Wei *et al*, 2013) who concluded in their papers that students use social websites for chatting and sharing files. Facebook, YouTube and Wikipedia are ranked as the most popular websites used by college students.

Moreover, the results of the questionnaires support what (Ning & Bao, 2010) stated in that email can motivate the students to improve their reading and writing skills.

Many students who participated in the questionnaire of the primary research found the social media and email experience enriching, and therefore reported high levels of interest.

Based on these findings, it was proposed that the any of OCG tools that the students found interesting should be implemented in teaching and learning.

9.3 Discussion of the findings of the students' perception of the secure SWFG tools

The quasi-experiment, which has been discussed in Chapter 5, revealed that secure SWFG can deliver a more suitable educative collaborative groupware in the class room. Furthermore, the students need to be motivated by their teachers in order to trust in the

OCG tools. The students were motivated and encouraged to use such tools but they need to trust the tools.

The overall findings from the student feedback confirmed the findings of the earlier primary research discussed in Chapter 4. The experiment found that the security and privacy of Skype may encourage the students to use it. However, Gmail, Facebook, and Wikis have a lack of usage and trust from the students because of the lack of security.

The findings from the experiment, the students' feedback, observation, and log files during the experiment provided evidence to support the proposal and its associated hypothesis that secure emails can increase usage and trust of email. Furthermore, they provided the basis for the development of a secure email framework (intervention) in order for email to be effective. This model was then tested through the evaluation of secure emails.

These results support Martin (1996) and Ning and Bao (2010) which state that email can simplify communication between students and teachers and can also be a motivating factor for students to improve their reading and writing skills. Moreover with respect to secure emails, the results support Dhanaraj (2013) who pointed out that "freedom of communication is being, issued and have become a threat to email communication society".

9.4 Discussion of the findings of the evaluation of the students' awareness towards secure email

The evaluation of the students' awareness of secure email in Bahrain and the UK revealed that Bahraini students often access webmail but not frequently and not for educational purposes, whereas the UK students use the university email frequently and for educational purposes. Furthermore, the evaluation indicated that students from both

countries have the same belief that email is secure when only the attachments are scanned. On the other hand this evaluation revealed that the respondents in both countries are not aware of security technologies, which help the emails to be trusted and secure. This led the researcher to conduct an intervention in which a secure email design model which was developed in order to critically examine secure email usage and awareness.

9.5 Discussion of the results of the secure email tracking model

This section discusses the results of the intervention, in which students logged their secure email usage awareness of attacks and the action taken.

9.5.1 Discussion of the results of the secure email usage

The descriptive analysis has shown that the participants in the UK and BAH use email rarely during the day but for both academic and non-academic purposes. It was noticed that both countries accessed their emails for academic more than non-academic, and that email access was more frequent in the UK. Also, the results revealed that the participants in the UK access both kinds of emails naming webmail such as Gmail, Hotmail, (and rarely Yahoo) as well as university emails. On the other hand, the participants in BAH access only webmail and mostly Hotmail.

9.5.2 Discussion of the results of the email attacks' awareness

The email attacks, awareness for academic and non-academic in both countries was tested by t-test. The results indicated that there was no difference between the means of all attacks in Bahrain and UK for both academic and non-academic purposes except for "spam" attacks against emails in BAH. This indicated that most of the participants receiving emails in BAH had more spam attacks in their non-academic emails.

9.5.3 Discussion of the results from the action taken against emails

With regard to the action taken against the attacks, the hypotheses results concluded that there was no difference between the means of all actions taken with academic and non-academic emails in BAH and UK apart from the "ignore" action. The research indicated that participants in BAH are not aware of such security attacks and then they ignore any attacks they face when accessing their emails.

Furthermore, It was noticed from the results of the hypotheses and from the qualitative analysis (interviews and observations) that the respondents from both countries are not aware of signing and encryption technology.

The results referred to above, together with the conclusions from this study Seem to support previous research, which has found that human awareness and education are needed in order to protect emails from any malicious attacks. (Jansson & von Solms, 2011) confirm this, as they stated "Security education, training and awareness programs have proved to be the most successful regarding protecting end users against malicious attacks". (Jansson & von Solms, 2011) support the previous results in that many of the emails end users do not pay attention to such awareness techniques.

Moreover Gerck, Ed. (2007) support the result of this intervention – that email users would rather use an insecure email system that is easy to use than a secure email system where even the help text Seems intimidating.

We concluded from this activity which is derived from Gerck, Ed. (2007) that the secure email system has to be easy to use when compared with simple, familiar, regular email systems. This is distinct from other secure email systems because If security settings are too tough or frustrating, users may give up on it altogether.

Siu Man Lui and Hui (2011) supported my conclusion in that they stated that "it is important to understand how knowledge affects security decisions especially when

education, training and awareness programs are one of the most suggested strategies to change human security behaviour."

9.6 Discussion of the results regarding the validation of the research framework

In this Chapter, the researcher conducted a one-shot case study (as identified earlier in the Chapter) to validate the contextual framework (which has resulted from the previous intervention as shown in the Fig 8.1) and to answer the research questions and test the hypotheses listed above. The following conclusions were driven from the hypotheses testing:

- Secure email and each of perceived ease of use and trust are positively correlated.
- Trusted email is positively related to perceived ease of use of the email.
- Perceived ease of use is positively related to perceived usefulness of the email
- Perceived ease of use is negatively related to actual usage of email.
- Perceived usefulness is negatively related to actual usage of email.

Thus, the framework depicted in Figure 8.1 has been validated for only hypotheses 1 to 4. In other words, the researcher can confirm that secure email and trusted emails leads to ease of use, which in turn lead to usefulness. Moreover, ease of use relates to usefulness which is already validated by (Hubona,2003). However, the result of this case study clashes with (Hubona,2003) in which the H5 and H6 were rejected. In other words ease of use and usefulness are significantly related, but the correlation is negative which cannot validate the framework. Thus, we can conclude that the research framework is not validated.

Moreover, descriptive analysis shows major of the participants indicated that they have used email for learning occasionally, and about one third (30.8%) rarely. However, 8.8%

of the participants used email for learning regularly. In addition to that, the most frequently used email by the participants was Hotmail (40.7%).

Quantitative and qualitative analysis indicated that the UOB sample were not aware of email what they use email for, or how to secure email. This was clear from interviews and observations which support the hypotheses analysis. The following limitations prevents the framework from being validated.

1. Lack of the students and teachers knowledge of security settings in their email;
2. The teachers do not motivate their students to use the email in the learning;
3. UOB administrators do not encourage the students and teachers to use UOB university email;
4. The researcher took time to explain to the students how to secure emails. This led the students to think that this was a lecture which made them feel bored
5. The researcher had difficulties finding a sample that could cooperate with her in order to facilitate the adjustment of the students' security settings;
6. Some of the students did not cooperate with the researcher in that they do not use the emails in the learning during the case study.

9.7 Contributions to Knowledge

The researcher has developed a framework derived from TAM theory and discussed in Chapter 8 and which has been tested in order to validate the framework based on email usage. The researcher chose the TAM model and modified it by adding new variables such as security and trust. The researcher discovered that Hypotheses 8.4 and 8.5 needed to be modified in a way that the ease of use and usefulness contributes to increase the actual usage of the email. The following are the new dimensions of email usage:

1. "Trust and security" used in this research can be used as measures to test the emails' usefulness and ease and of use.

2. According to the students' perception in UOB, signing and encryption seem to be not important for secure email as the email security settings enabled are enough to feel comfortable with ease when access their emails. Therefore, it is not necessary to include such technologies in the IT curriculum as webmail providers have simple security settings and the students can fix them easily.
3. Ease of use and usefulness does not always lead to actual email usage.
4. Neither perceived ease of use or usefulness are affected by the users' choice of webmail provider.

9.7.2 New definition of email usefulness

Email usefulness can be defined as a combination of trusted and secure email, which provides high levels of ease of use. This definition is based on the research framework depicted in Figure 8.1.

9.7.3 Developing SWFG model for CSCL

The researcher has developed a SWFG model with dimensions of security, trust, privacy and safety, as explained in Chapter 5, which can deliver more suitable educative collaborative groupware in the classroom.

9.7.4 New secure email model

The researcher has developed a secure webmail instructional model (explained in Chapter 8) which was the practice applied in the quasi-experiment to validate the research framework. The model was built to validate the framework which was developed based on the TAM model. The model has strategies and instructions about how to manage the usage of email in the learning. The researcher succeeded to test the framework using this model and it was easy for IT students to follow and apply. Moreover, it allows the students to learn how to manage their email.

9.8 Dissemination of knowledge gained

Throughout the course of this study, the researcher was able accumulate a great deal of knowledge. Moreover, the researcher had the opportunity to publish one conference paper and presented at another conference, all of which are highlighted below.

1st Publication: Conference paper

Aladraj, R. & Joy, M. (2013) Security and Collaborative Groupware Tools in Education: A Case Study at the University of Bahrain. e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity" , 2013 Fourth International Conference on, Date of Conference:7-9 May 2013, Page(s):421 - 426, INSPEC Accession Number:14115721,ConferenceLocation Manama,DOI:10.109/ECONF.2013.56

Publisher:IEEE

2nd dissemination: Conference presentation

Aladraj, R. (2012) Application of Security to Cloud-Based Groupware Tools in Education: A presentation in the conference Colla12, Venice, Italy.

Future publications:

"New dimensions of secure webmail usefulness in the learning" has been submitted to the econf2015 which will be held on October 2015.

9.9 Limitations of the study

Several limitations may be commented on regarding the experiment. First of all, the research was only conducted at the University of Bahrain (UOB), whereas including other universities in Bahrain might provide a better representation of Bahraini students. This would have enabled the researcher to work towards more comprehensive findings, representative of students all over Bahrain. Furthermore, only first-year students at UOB participated in this study. A wider study would comprise students of different stages of

their studies.

A further limitation of the study may be the validity and reliability of the investigations conducted. However, the researcher has attempted to minimize the impact of this investigation on the students by using multiple methods of data collection to complete this study. For example, interviews, log files and observations were widely used throughout to ensure that data was collected from different sources.

Also, it is known that in some studies the 'novelty effect' can influence how respondents react to a system (Al Khaili, 2012). It is the author's view that in this study some of the students have had a lack of motivation towards OCG tools and discouragement from their teachers.

A final comment on limitations has to do with the researcher' personal circumstances. The researcher has to do the experiments in Bahrain as the sample of all the experiments are Bahraini students, It was difficult for the researcher to travel for each experiment and the activity as she was living in the UK during the PhD period. The researcher was obliged to invest her own skills, time and money. Moreover, the researcher has children and it was difficult to leave them alone in the UK.

9.10 Significance of the Study

This research has effect and significance on different factors affecting teaching and learning with OCG tools especially email. These effects are described as follows:

9.10.1. For the researcher

The completion of this research has enabled the researcher to contribute in three major areas:

1. The researcher has contributed through a production of an innovative SWFG model which can be used as innovative model for teaching and learning.

2. Moreover, this study helped in solving the lack of communication between the teachers and the students in UOB who were otherwise prevented from face to face meetings due to time constraints.
3. The researcher identified the perceptions of the IS students in UOB towards SWFG usage and security, so she can know how to deal with them.
4. The researcher has contributed through the effective development of a new instructional mode for secure email usage that could be adapted to enhance teaching in other areas.

9.10.2 For teachers

UOB teachers can benefit greatly from this study as a more effective teaching method which can be available in their teaching practice. This will help to motivate a large number of students to use the OCG tools. In turn, this will make the teaching process more enjoyable for the teachers. Likewise, the email usage should help them to overcome some of the time pressures associated with the academic workload.

9.10.3 For students

This study will be beneficial for the IT students as the new proposed method and associated application would appear to be more enjoyable and engaging methods to support educational process. The email usage model developed should enable students to independently use emails in their learning, more easily and faster. It should also allow them to have more privacy so that trial and error, failing tests and assignment, and asking embarrassing questions can all be experienced without disclosure. The students can use OCG in learning methods whenever they need and want, as well as in a variety of places.

9.10.4. For UOB

The outcomes of this study should help to improve the learning and teaching in UOB. Applying SWFG and email usage models may improve effectiveness and efficiency for both students and teachers in learning and teaching. This, in turn, can help to overcome the shortage of time for the teachers in dealing with the large number of students. It should also allow students to be active rather than passive in which that are subjected to an action without responding or initiating action in return.

9.11 Recommendations

The recommendations are informed from a combination of the comments, feedback and data analyses obtained as part of this study. The recommendations are focused on two main areas and are set out in the following sections.

9.11.1 For UOB

UOB are recommended to utilize OCG tools to overcome the current overcrowding of classes and the teachers' limited time. Email should be used for communication between the teachers and the students in the learning with the presentation media and teaching board. In doing so, the IT center in UOB must motivate the teachers and the students to use university email by providing them with any help at any time and guarantee fixing the security settings for the students in order to encourage the students to use them. Moreover, the E-learning center in UOB must help the teachers to use the OCG tools with the e-learning profiles like Webct and Model.

9.11.2 For UOB teachers

The following recommendations should be applied to provide teachers with teaching skills.

- UOB teachers are recommended to enrol on workshops for using OCG tools and

increase their awareness of such tools;

- Teachers should train the students at the beginning of the course on how to use the SWFG model and instructional email usage model in order to use them in their teaching.
- Teachers must be up-to-date about the innovative OCG tools in the market to apply them in their curriculum;
- Teachers should encourage and motivate students to use OCG tools in their learning and secure emails for communication such as assignment submission, project group work, and enquires.
- Teachers should encourage the students to download the OCG tools and webmail on their mobile.

9.12 Curricula of IT courses

The curricula of IT courses have to be changed to include OCG tools approaches, including secure email usage. New course curricula must include theoretical and practical aspects of security and OCG tools usage concepts. To achieve this objective, the following recommendations should be taken into consideration:

- UOB are suggested to add OCG tools in IT courses such as (BIS 202, ITBIS 101 and BIS 105) instead of teaching them office applications which are already studied in their schools.
- Include UOB Outlook email in the curricula;
- IT Centre in UOB must help the teachers by providing students with any help at any time, and guarantee fixing the security settings for the students in order to encourage students to use them;
- E-learning centre in UOB must help the teachers to use the OCG tools with the

e-learning profiles like Webct and Model;

- IT and E-learning centre must follow up the teachers and the students about their email usage and progress with using up-to-date OCG tools;

9.13 Suggestions for future research

Researchers are recommended to further test this study with different students from different colleges in UOB and at other universities in Bahrain, in order to validate the research framework, particularly with the email usage factor. Furthermore, with other innovative OCG tools, other researchers could test the SWFG model. More investigation might also be carried out into whether the new instructional model could be applied to other areas than IT colleges.

9.14 Conclusion

The aim of this study was to identify and develop efficient models for using OCG tools in teaching and learning, especially with UOB students. The findings of this investigation, together with the model and hypotheses testing, have enabled the researcher to successfully achieve this aim.

The study was able to empirically demonstrate, and partly validate the email usage framework. Moreover, it has developed a new design model for its successful implementation.

The overall finding of this study is that security and trust of email enhances the ease of use and usefulness of email within learning. These results are very encouraging for the use of secure email in learning. The main results have then been translated into actionable recommendations to be implemented, so as to improve the adoption of OCG tools within learning environments. The study has also demonstrated that the OCG tools are a suitable solution for the lack of communication between the teachers and the

students in the learning environment, and can help to keep students up-to-date with educational technologies, and can use the independently when their security settings are correctly adjusted.

References

Adeyinka, O. (2008) Internet Attack Methods and Internet Security Technology. i*n Modeling & Simulation. AICMS 08. Second Asia International Conference.* Kuala Lumpur, 13-15 May, 2008. IEEE.77-82.

Alkhalili, K.(2012) Validity of the instrument.[Interview].4th March 2012.

Alkhalili, K.(2014) Validity of research framework.[Interview].15th April 2014.

Almadhoun, N. M., Dominic, P. D. D. & Lai Fong, W. (2011) Perceived security, privacy, and trust concerns within Social Networking Sites: The role of Information sharing and relationships development in the Malaysian Higher Education Institutions' marketing. in *Control System, Computing and Engineering (ICCSCE)*. IEEE.426-431.

Andrew, M. (2003) Should we be using web-based learning to supplement face-to-face teaching of undergraduate. in *6* International Conference on Computer-Based Learning in Science.* 2003. Nicosia:University of Cyprus.

Aladraj, R. & Joy, M. (2013) Security and Collaborative Groupware Tools in Education: A Case Study at the University of Bahrain. in *e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity conference* , Manama, 2013.IEEE.421-426.

AlAmmal, H. (2014) *Information Technology College*. [online] Available from:http://www.uob.edu.bh/english/pages.aspx?module=pages&id=2605&SID=139.[Accessed: 17th May 2015]

Andrew, M. (2003) *Should we be using web-based learning to supplement face-to-face teaching of undergraduate*. [online] Available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.521.1697. [Accessed: 20th June 2012]

Baker, K., Greenberg, S. & Gutwin, C. (2002) *Empirical development of a heuristic evaluation methodology for shared workspace groupware. Computer supported cooperative work.* 2002. New York:ACM.

Babbie, E. R. (1990). *Survey research methods (2nd ed.)*. Belmont, CA: Wadsworth.

Bergeron, E. (2000) The Difference Between Security and Privacy. [online]. Available from: http://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html .[Accessed: 20th December 2014]

Bourimi, M., Kuhnel, F. & M.Haak, J. (2009) Tailoring collaboration according privacy needs in real-identity collaboration systems. in: 15th International Workshop, C. Groupware: Design, Implementation, and Use. *Groupware: Design, Implementation, and Use.* Berlin: Springer.

Brush, A. J. B. & Borning, A. (2005) Today' Messages: Lightweight Support for Small Group Awareness via Email. in: System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference. Hawaii, 03-06 Jan. 2005.IEEE.p.16a

Businessdictionary.2014.Authorization.[online]. Available from: http://www.businessdictionary.com/definition/authorization.html#ixzz3C94ApQxE.[accessed:2oth December 2014]

Birley, G. & Moreland, N. (1998). *A practical guide to academic research*. London: Kogan page Limited.

Branwell,B. & Lane, B. (2000) Tourism collaboration and partnership: politics, practice and sustainability. [online] Available from: http://books.google.co.uk/books [Accessed: 28 August 2011].

Cailleux, L., Bouabdallah, A. & Bonnin, J. M. (2014) A confident email system based on a new correspondence model. in: *Advanced Communication Technology (ICACT)*. Pyeongchang, 16-19 Feb. 2014. IEEE.489-492.

Campbell, D.T., & Fiske, D.W, *(1959).* Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, 56(2).81 -105.

Chade, P. (2011) *The difference between secrecy and privacy as security concepts*. [online] Available from: http://www.techrepublic.com/blog/it-security/the-difference-between-secrecy-and-privacy-as-security-concepts/ [Accessed: 20th December 2014]

Crain, J., Opyrchal, L. & Prakash, A. (2010) Fighting Phishing with Trusted Email. in: *Availability, Reliability, and Security*, Krakow, 15-18 Feb. 2010. IEEE.462-467.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Approaches.education researcher*. 4th Ed.California: Sage.

Creswell,J. & Dana L. Miller (2000). *Determining Validity in Qualitative Inquiry*. [Online] Available from: http://people.ucsc.edu/~ktellez/Creswell_validity2000.pdf. [Accessed: May 2013].

Dabbagh, N. (2002) *Web-based course management tools, In Educational technology*. [online] Available from: http://mason.gmu.edu/~ndabbagh/wblg/WBCMT-encyclopedia entry.htm [Accessed: 20the December 2014].

Danyaro, K. U., Jaafar, J., De Lara, R. A. A. & Downe, A. G. (2010) An evaluation of the usage of Web 2.0 among tertiary level students in Malaysia. in: *Information Technology (ITSim)*. Kuala Lumpur,15-17 June 2010.1-6.

Dembovskaya.S (2009) *Task-based instruction:the effect of motivational and cognitive pre-tasks on second language oral french production.* A Thesis Submitted in partial fulfilment of the Requirements of University of Iowa for the degree of Doctore of Philosophy. University of Iowa.Dhanaraj, S. & Karthikeyani, V. (2013) A study on e-mail image spam filtering techniques. in: *Pattern Recognition, Informatics and Mobile Engineering (PRIME)*, 2013.IEEE.49-55.

Dillenbourg P. (1999) What do you mean by collaborative leraning?. In P. Dillenbourg (Ed) *Collaborative-learning: Cognitive and Computational Approaches.* [online] Available from: http://tecfa.unige.ch/tecfa/publicat/dil-papers-2/Dil.7.1.14.pdf. Oxford: Elsevier.

Dillman, D. A. (2000). *Mail and Internet surveys: The tailored design method*, 2nd ed, New York, NY: John Wiley & Sons.

D'Agostino,C. (2013). Collaboration as an Essential School Social Work Skill. *Oxford Journals.* [Online] Available from: http://cs.oxfordjournals.org/content/35/4/248.extract#.[Accessed:22 Novemeber 2014]

McKnight.D & Choudhury.V & Kacmar.C (2002). *Developing and Validating Trust* Measures for e-Commerce.*Information system Research.* [Online]. Available from: https://www.msu.edu/~mcknig26/Measures.pdf.[Accessed: 22 December 2014].

Ebay. (2007) *Using ebay Toolbar's Account Guard*. [online] Available from: http://pages.ebay.com/help/confidence/account-guard.html .[Accessed: 12 December 2014]

Foswiki (2010) *Wiki - culture, concepts and principles.*[Online] Available from: http://foswiki.org/System/WikiCulture.[Accessed: 24 June 2014].

Garcia, O., Favela, J. & Machorro, R. (1999) Emotional awareness in collaborative systems. in *String Processing and Information Retrieval Symposium, and International Workshop on Groupware*. IEEE.296-303.

Goh Wei, W. (2012) The use of wiki to facilitate critical thinking. in *Teaching, Assessment and Learning for Engineering (TALE)*. Hong Kong, 20-23 Aug. 2012. IEEE. H3C-1-H3C-3.

Gerck, E. (2007) Secure Email Technologies X. 509/PKI, PGP, IBE and Zmail. *Corporate Email Management. Corporate Email Management*, CFAI University Press.

Ghafoor, A., Muftic, S., Schmo, x & lzer, G. (2009) *CryptoNET:* Design and implementation of the Secure Email System. in *Security and Communication Networks (IWSCN), 2009 Proceedings of the 1st International Workshop*. Trondheim,20-22 May 2009. IEEE.1-6.

Gill, J. and Johnson, P. (1997). *Research Methods for Managers*, (2nd ed.), Paul Chapman Publishing, London.

Google. (2007.) [online] Available from: http://www.google/tools/firefox/safebrowsing/. [Accessed: 12 December 2014]

Gunnlaugsdottir, J. (2003) Seek and you will find, share and you will benefit: organising knowledge using groupware systems. *International Journal of Information Management*, 23 (5). 363-380.

Gutwin, C. & Greenberg, S. (1999) *The effects of workspace awareness support on the usability of real-time distributed groupware*. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 6 (3).243-281.

Gutwin, C., and Greenberg, S. (2001) A Descriptive Framework of Workspace Awareness for Real-Time Groupware. *Computer Supported Cooperative Work*, Kluwer Academic Press.

Hairsine, K. & Karbasova, N. (2013) *Think Skype is safe?* . [online] Available from: http://akademie.dw.de/digitalsafety/think-skype-is-safe-think-again/.[Accessed:1July 2013]

He, Y.-z., Cheng, C., Xu, Q.-s. & Yang, L.-h. (2014) A research on methods and applications of case study in public administration. in *Management Science & Engineering (ICMSE)*, Finland, 17-19 Aug. 2014. IEEE.1977-1982.

Hernandez, R., Amado-Salvatierra, H. R., Guetl, C. & Smadi, M. (2012) Facebook for CSCL, Latin-American Experience for Professors. in *Advanced Learning Technologies* (ICALT), Rome, 4-6 July 2012.IEEE. 327-328.

Hewitt, A. & Forte, A. (2006) Crossing boundaries: Identity management and student/faculty relationships on the Facebook in *Computer Supported Cooperative Work Conference.Canada,* November 4-8.ACM.

Hubona, G. S. & Burton-Jones, A. (2003) Modeling the user acceptance of e-mail. in *System Sciences, Proceedings of the 36th Annual Hawaii International Conference* . 6-9 Jan. 2003.IEEE.

Jansson, K. & von Solms, R. (2011) Simulating malicious emails to educate end users on-demand. in *Web Society (SWS), 2011 3rd Symposium*. Port Elizabeth, 26-28 Oct. 2011. IEEE.74-80.

Javanmardi, S., Ganjisaffar, Y., Lopes, C. & Baldi, P. (2009) User contribution and trust in Wikipedia.in *Collaborative Computing: Networking Applications,* Washington, 11-14 Nov 2009. IEEE.1-6.

Jingbo, Z. & Yueliang, Z. (2010) Design and application of the special study website based on wikispace. in *Networked Computing (INC), 2010 6th International Conference*. Gyeongju, 11-13 May 2010,Korea (South).IEEE.1-4.

Johnson, G. M. (2005) Student Alienation, Academic Achievement, and WebCT use. *Educational Technology and Society*, 8(2).179-189.

Judele, R., Tsovaltzi, D., Puhl, T. & Weinberger, A. (2014) Collaborative Learning in Facebook: Adverse Effects of Individual Preparation. in *System Sciences (HICSS), 2014 47th Hawaii International Conference*.6-9 Jan. 2014,Waikoloa. IEEE.1616-1624.

Keengwe, J., Onchwari, G. & Wachira, P. (2008) The Use of Computer Tools to SupportMeaningful Learning. *AACE Journal*, 16 (1).77-92.

King, D. J. (2010) An investigation into the role of a wiki in supporting collaborative learning activities. A Thesis Submitted in partial fulfilment of the Requirements of The Open University for the degree of Doctore of Philosophy. The Open University.

Leelathakul, N. & Chaipah, K. (2013) Quantitative effects of using facebook as a learning tool on students' performance. in *Computer Science and Software Engineering (JCSSE), 2013 10th International Joint Conference.* 29-31 May 2013, Maha Sarakham. IEEE.87-92.

Leedy, P. D. (1997). *Practical research: planning and design* (6th ed.), Upper Saddle River, NJ: Prentice-Hall, Inc.

Littleton, K. & Light, P. (1999) *Learning with computers analysing productive interaction*. London: Routledge.

Lindberg, K. & Jensen, C. D. (2012) Collaborative trust evaluation for wiki security. in *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference*. Paris, 16-18 July 2012.IEEE.176-184.

Lipponen, L. (2002) Exploring foundations for computer-supported collaborative learning. in *Proc. of CSCL 2002*.ACM.72-81.

Liu, C-H. (2010) The comparison of learning effectiveness between traditional face-to-face learning and e-learning among goal-oriented users. in *Digital Content, Multimedia Technology and its Applications (IDC), 2010 6th International Conference*. Seoul,16-18 Aug. 2010.IEEE. 255-260.

Lv, J., Zhou, W. & Wang, X. (2010) Design and evaluation of a wiki-based collaborative learning environment for colleges computers compulsory education. in Computer Science and Education (ICCSE), *2010 5th International Conference*. Hefei, 24-27 Aug. 2010. IEEE.695-699.

Malcolmson, J. (2009) What is security culture? Does it differ in content from general organisational culture? in *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conferenc.* Zurich, 5-8 Oct. 2009.IEEE.361 - 366.

Marotta,L. (2006) *Utilizing the full advantages of groupware applications to boost team collaboration.* [online] Available from: http://www.web-conferencing-zone.com/advantages-of-groupware-applications.htm. [Accessed:20th December 2014]

Martin, F. & Noonan, D. (2010) Synchronous technologies for online teaching. in Technology for Education (T4E), *2010 International Conference*. Hyderabad, 18-20 July 2012. IEEE.1-4.

May,M. & George,S. (2011) Privacy Concerns in E-learning: Is Using Tracking System a Threat?.*International Journal of Information and Education Technolo*gy, 1(1).

Mondofacto.(2000). [online].Available from: http://www.mondofacto.com/facts/dictionary?content+validity .[Accessed:2014]

Milne, J. (1999). Evaluation Cookbook, Learning Technology Dissemination Initiative, Aberdeen University.[Online]. Available from: http://www.icbl.hw.ac.uk/ltdi/cookbook/info_questionnaires [Accessed: 2012]

Nance, E. (1994) The Conical Methodology and the evolution of simulation model development .*Annals of Operations Research*.53(1).1-45.

Neuman, W. L. (2000). *Social research methods: Qualitative and quantitative approaches* (4th ed.). Boston: Allyn & Bacon.

Nemec, L., Holbl, M., Burkeljca, J. & Welzer, T. (2011) Facebook as a teaching tool. in *EAEEIE Annual Conference (EAEEIE), 2011 Proceedings of the 22nd*. Maribor,13-15 June 2011.IEEE.1-4.

Ning, Z. & Bao, H. (2010) Research on Computer Technology for E-learning in Higher Education. in *e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E '10. International Conference*. Sanya, 22-24 Jan. 2010. IEEE.295-298.

Newsroom.(2014). Statistics.[online]. Available from: http://newsroom.fb.com/key facts.[Accessed:12 December 2014]

Papert, S. (1992) *The children's machine.* New York*:* BasicBooks New York:

Parker, M. & Media, D. (2014) Can you trust Skype?. [Online] Available from: http://smallbusiness.chron.com/can-trust-skype-69644.html.[Accessed:12 December 2014].

Pearson, S. & Yee, G. (2013) *Privacy and Security for Cloud Computing*. Springer.

Pentafronimos, G., Karantjias, A. & Polemi, N. (2011) Open issues on privacy and trust in collaborative environments. in *Computers and Communications (ISCC), 2011 IEEE Symposium on. Kerkyra,* June 28 2011-July 1 2011.IEEE.876-880.

Perez-Mateo, M. Tools for Collaborative Learning: The Use of Wiki. in *Intelligent Networking and Collaborative System*s, 2009. INCOS '09. International Conference. Barcelona, 4-6 Nov. 2009.IEEE.405-408.

Raitman, R., Augar, N. & Zhou, W. (2005) Employing Wikis for Online Collaboration Collaboration in the E-Learning Environment: Case Study. in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference*. Sydney, 4-7 July 2005. IEEE.142-146.

Robison, C., Ruoti, S., van der Horst, T. W. & Seamons, K. E. (2012) Private Facebook Chat. in *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference and*

*2012 International Conferenc*e on Social Computing (SocialCom). Amsterdam,3 -5 Sept. 2012.IEEE.451-460.

Rouse, M. (2005a) *Groupware*. [online] Available from: http://searchdomino.techtarget.com/definition/groupware .[Accessed 20th December].

Rouse, M. (2014b) *digital-signature*. [online] Available from: http://searchsecurity.techtarget.com/definition .[Accessed: 12 December 2014]

Rousseau, D. , Sitkin,S. Burt,R. & Camerer, C. (1998) Not so different after all: a cross-discipline view of trust. *Academy of Managemnet Review,* 23 (3): 393-404.

Ruoman, Z. & Chuan, Z. (2009) A Framework for Collaborative Learning System Based on Knowledge Management. in *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop*. Wuhan, Hubei, 7-8 March 2009.IEEE.733 - 736.

Salem, O., Hossain, A. & Kamala, M. (2010) Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks. in C*omputer and Information Technology (CIT), 2010 IEEE 10th International Conference*.Bradford, June 29 2010-July 1 2010. IEEE. pp.1418-1423.

Sheldon, P. (2008) The relationship between unwillingness-to-communicate and students' Facebook use. *Journal of Media Psychology*. 20 (2): 67–75.

Siu Man, L. & Hui, W. (2011) The effects of knowledge on security technology adoption: Results from a quasi-experiment. in *Proceedings of the 5th International Conference on New Trends in Information Science and Service Science*. Macao,24-26 Oct. 2011.IEEE. 328-333.

Smith, C. (2014) By numbers:200+ amazing Facebook user & demographic statistics. [online] Available from: http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/ .[Accessed: 12 December 2014]

Solic, K., Sebo, D., Jovic, F. & Ilakovac, V. (2011) Possible decrease of spam in the email communication. in *MIPRO, 2011 Proceedings of the 34th International Convention. Opatija*, 23-27 May 2011.IEEE.1512-1515

Soon, L. & Fraser, C. (2011) Knowledge activities in distance education online group work. in 3*rd International Conference on Communication Software and Networks (ICCSN)*. Xi'an, 27-29 May 2011.IEEE. 364-369.

Stoy, A. (2010) *Disadvantages of Groupwork collaboration Software*. [online] Available from: http://www.brighthub.com/office/collaboration/articles/78665.aspx .[Accessed 1 June 2012].

Strnad, M. & Rugelj, J. (2010) Assessment of wiki-supported collaborative learning in higher education. in *Information Technology Based Higher Education and Training (ITHET), 2010 9th International Conference*. Cappadocia, April 29 2010-May 1 2010.IEEE.79-85.

Suleman, S. (2003) *Use of Communications Tools within VLE*. [online] Available from: http://ferl.becta.org.uk/display.cfm?resID=5497. [Accessed: 12 December 2014]

Szedmina, L. & Pinter, R. (2010) *Experiences from using Skype in language teaching*. in *Intelligent Systems and Informatics (SISY), 2010 8th International Symposium.* Subotica, 10-11 Sept. 2010. IEEE.449-452.

Terpstra.L. (2002) A security model for the work space groupware architecture. [Online] Available from: http://symbiosis.rmc.ca/pub/terpstra-meng-thesis-2002.pdf . [Accessed: 2 December 2011]

Thao, L. & Quynh, L. (2002) The nature of learners' email communication. in *Computers in Education, 2002. Proceedings. International Conference.* 3-6 Dec. 2002.IEEE.468-471.

Treepuech, W. (2011) The application of using social networking Sites with available online tools for teaching and learning management. in *IT in Medicine and Education (ITME), 2011 International Sympo*sium. Cuangzhou, 9-11 Dec. 2011. IEEE.326-330.

Trentin, G. (2009) Using a wiki to evaluate individual contribution to a collaborative learning project. *Journal of Computer Assisted Learning*.25.43-55.

Techtarget. (2014). history-of-email .[Online]. Available from: http://searchsecurity.techtarget.com/definition/authenticationl.[Accessed:2014]

Trinidad, S. (2003) *Working with Technology-rich Learning Environments: Strategies for Success.* Technology-Rich Learning Environments A Future Perspective. New Jersey: World Scientific.

Travellerspoint. (2014). [online].Available from: http://www.travellerspoint.com/guide/Bahrain. [Accessed: 12 December 2014]

Tsoulis, M., Tsolakidis, C. & Mitkas, K. (2013) Collaborative learning using google facilities. in I*nteractive Collaborative Learning (ICL), 2013 International Conference*. Kazan, 25-27 Sept. 2013. IEEE. 577-582.

UOB.(2012).FastFacts.[online].Available from: http://www.uob.edu.bh/english/pages.aspx?module=pages&id=2990&SID=312 .[Accessed 12 December:2014].

Vicomsoft.(2014). history-of-email .[Online]. Avalibale from: http://www.vicomsoft.com/learning-center/history-of-email.[Accessed: 12 December 2014]

Worksharing, 2009. CollaborateCom 2009. 5th International Conference on. Washington, DC.IEEE. 1-6.

Webb, E. J., Campbell, D. T., Schwartz, R. D., and Sechrest, L. (1966). *Unobtrusive Measures: Nonreactive Measures in the Social Sciences*. Chicago: Rand McNally.

Wei Wei, G., Jer Lang, H. & Kheng Swee, G. (2013) Students' behavior and perception of using Facebook as a learning tool.in *Computer Science & Education (ICCSE), 2013 8th International Conference*. Colombo, 26-28 April 2013.IEEE.731 - 736.

Wikipedia.(2012).Skype. [Online] Available from: http://en.wikipedia.org/wiki/Skype.[Accessed: 21 January 2014]

Wikipedia (2014a).Webmail.[Online]. Available from: http://en.wikipedia.org/wiki/Webmail [Accessed:20 January 2014]

Wikipedia (2014b).Email.[Online] Available from: http://en.wikipedia.org/wiki/Email. [Accessed:20 January 2014]

Wikipedia (2014d).User_account.[Online] Available from: http://en.wikipedia.org/wiki/Wikipedia:User_account_security [Accessed:27January 2014]

Yu-ching, C. (2011) Learning styles and adopting Facebook technology. in *Technology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET '11*. Portland, July 31 2011-Aug. 4 2011.IEEE. 1-9.

Zhengjun, W., Mingzhang, Z. & Longlong, L. (2008) The Impact and Influence of Educational Technology Practice on Chinese Educational Culture. in *Knowledge Acquisition and Modeling, 2008. KAM '08. International Symposium*. Wuhan, 21-22 Dec. 2008.IEEE.476-480.

Zuckerberg, M. (2014). [online]. Available from: newsroom.fb.com/key-facts.[Accessed: 12 December 2014]

Appendices

Appendix A

Questionnaire-1

Electronic questionnaire refere to:
(http://www2.warwick.ac.uk/fac/sci/dcs/research/edtech/surveys/resala,2012),

University of Warwick
Computer Science Department
Questionnaire -1

Security issues and Collaborative groupware questionnaire

I am a PhD student and I am interested in security issues in collaborative groupware. The purpose of this activity is to explore the student perceptions of security that relate to the different collaborative tools. The data I receive will be kept confidential and will be stored anonymised. The data will only be seen by myself and my supervisor, Dr.Mike Joy. The Department's ethical procedures have been followed, and ethical consent has been granted for this

Section -1:Personal information

1-Name(*optional):* _____

2-Age:(*optional*) _____

3-Year: ☐ 1st ☐ 2nd ☐ 3rd ☐ 4th

4-Course: ☐ CS ☐ CBS ☐ Discrete Math ☐ Other Please specify: _____

5-Which learning management systems have you used? Tick all that you apply.

☐ Moodle ☐ Sakai ☐Blackboard ☐Other Please specify: _____

Section-2: Experience of OCG usage

6- For each of the following, express your feeling about the tool.

***Note**: Effective means helping people increase their productivity through the collaboration and sharing of information.*

	Very effective	**Effective**	**Neither effective nor ineffective**	**Not effective**	**Completely ineffective**	**I have not used this tool**
a) Instant messaging	☐	☐	☐	☐	☐	☐
b) Social media (including Facebook)	☐	☐	☐	☐	☐	☐
c) Forums	☐	☐	☐	☐	☐	☐
d) Email	☐	☐	☐	☐	☐	☐
e) Shared whiteboard	☐	☐	☐	☐	☐	☐
f) Audio/video conference (Including Skype)	☐	☐	☐	☐	☐	☐
g) Blogs	☐	☐	☐	☐	☐	☐
h) Calendaring(e.g.outlook,Google calendar..)	☐	☐	☐	☐	☐	☐
i) Wikis	☐	☐	☐	☐	☐	☐
j) Document sharing	☐	☐	☐	☐	☐	☐
k) Telephony(not online)	☐	☐	☐	☐	☐	☐
l) Other	☐	☐	☐	☐	☐	☐

Please Specify: _____

Section-3: awareness of OCG tools security technology

7- Which of the following key features can provide benefits for you? Tick all that apply.

☐Data storage ☐Communication enablement ☐Problem solving Capabilities

7- If you are communicating with another person using collaborative tools, then "**authentication**" means assurance that the person who are communicating with in fact who they claim to be.

a-List three tools that you think have good authentication

_____

_____

_____

b-List three tools that you think have poor authentication

_____

_____

_____

8-Collaborative groupware tools keep a record of activities that the users have done ("Logs"). These logs may be confidential to the administrator, or may be publicly viewed by other users. Which of the approaches do you think appropriate?

☐ Confidential ☐ Public

-In either case please indicate your reasons?

_____

9-Which of the following security solutions are deployed in your home environment? Tick all that apply.

☐ Firewall ☐ Antispyware ☐ Spam filter ☐ Other Please specify: _____

10a-The following security technologies may be used, either directly or indirectly, to support the process of authentication. Which of the following you are familiar with?

☐SSL protocol ☐Packet Filtering ☐ Telnet protocol ☐ Protected Passwords ☐I do not know

10b- Which of the following security technologies you have used in your home environment?

☐SSL protocol ☐Packet Filtering ☐ Telnet protocol ☐ Protected Passwords ☐I do not know

Note: Protected passwords allow users to authenticate themselves to any message store when using insecure network without any risk.

11-Which of the following type of assessments do you prefer in doing your exams.

☐ E-exam ☐Paper-based

12- If a collaborative tool is used, a lot of information may or may not be stored and preserved. Which of the following types of information does a teacher need to preserve in order to deliver a course efficiently (using a collaborative tool).Tick all that apply.

☐ Students submitted assignments ☐ messaging history ☐Shared whiteboard

☐ grades awarded for submitted assignments ☐ Personal data (e.g.Address,Age,..etc)

☐Collaborative data(e.g. contents of messages) ☐ Other Please specify: _____

Thank you for taking the time to fill in this questionnaire.

Questionnaire-2

Questionnaire 2

University of Warwick
Computer Science Department
Questionnaire no.2-a
Resala Aladraj, PhD candidate

Group _____

I am a PhD student and I am interested in security issues in collaborative groupware tool usage. The purpose of this activity is to explore student perceptions of Online Collaborative Groupware (OCG) tool usage and their motivation towards secure usage. The data I receive will be kept confidential and will be stored anonymised. The data will only be seen by myself and my supervisor, Dr.Mike Joy. The Department's ethical procedures have been followed, and ethical consent has been granted for this questionnaire.

Section I: Personal information

1. Name (*optional):* _____
2. Age (*optional*): _____
3. Department: □ CS □ CE □ IS □ Other Please specify: _____
4. Year: □ 1st □ 2nd □ 3rd □ 4th
5. Course code: _____ Instructor_____ Date _____
6. Your secondary school: _____

Section II: Information about your experience of OCG tools.

Online Collaborative Groupware (OCG) is a system in which two or more students can share resources together in order to meet objectives that could not be met individually.

1. Which of the following Online Collaborative Groupware SWFGare you using as part of your **learning activities**? Tick all that apply.

	Home	University
Email	□	□
Facebook	□	□
Twitter	□	□
Wikis	□	□
Skype	□	□
Other	□	□

Please specify _____

2. Which activities are you doing with the tools you checked in Q1 as part of your **learning activities**? Tick all that apply.

Chatting/Discussion	□
Assignment submission	□
Quizzes	□
Document sharing	□

Video conferencing □

Other □

Please specify_____

3.On average, how many hours a day do you use the tools in Q1 **for learning activities**? Check one box only for each tool.

	I do not use it	Less than 1hr	Greater than or equal to 1 hr but less than 2 hrs	Greater than 2 hrs
Email	□	□	□	□
Facebook	□	□	□	□
Twitter	□	□	□	□
Wikis	□	□	□	□
Skype	□	□	□	□
Other	□	□	□	□

Please specify_____

Section III:Trust

4. Express your personal feelings while you are using those tools for learning activities. Tick all that apply.

Ease of use	Afraid	Worried	Pleased	Motivated

Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

5. How secure do you think those tools are? Check one box only on each row.

Secure means that information shared by the tool will only be accessible to those for whom it is intended.

	Very secure	Secure	Neither secure nor unsecure	Unsecure	Not secure at all
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

6. How safe to use do you think those tools are? Check one box only on each row.

Safe to use means the tool is protected from harm such as viruses, spyware, etc..

	Very safe	Safe	Neither safe nor unsafe	Unsafe	Not at all safe
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

7. How much privacy do you think these tools offer when being used for **learning activities**? Check one box only on each row.

Privacy: the ability of an individual or group to isolate information about themselves and thereby reveal themselves selectively.

	Has strong privacy	Has privacy	Neutral	Has little privacy	Has no privacy at all
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐

Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

8. Would you like to use SWFGin future **for learning activities** and why? Explain your answer.

Yes ☐ No ☐

_____

_____

End of the questionnaire

Group _____

University of Warwick
Computer Science Department
Questionnaire no.2-b
Resala Aladraj, PhD candidate

I am a PhD student and I am interested in security issues in collaborative groupware tool usage. The purpose of this activity is to explore student perceptions of Online Collaborative Groupware (OCG) tool usage and their motivation towards secure usage. The data I receive will be kept confidential and will be stored anonymised. The data will only be seen by myself and my supervisor, Dr.Mike Joy. The Department's ethical procedures have been followed, and ethical consent has been granted for this questionnaire.

Section I: Personal information

7. Name (*optional):* _____
8. Age (*optional*): _____
9. Department: □ CS □ CE □ IS □ Other Please specify: _____
10. Year: □ 1st □ 2nd □ 3rd □ 4th
11. Course code: _____ Instructor_____ Date _____
12. Your secondary school: _____

Section II: Information about your experience of OCG tools.

Online Collaborative Groupware (OCG) is a system in which two or more students can share resources together in order to meet objectives that could not be met individually.

1-Which of the following Online Collaborative Groupware OCG tools are you using as part of your **learning activities**? Tick all that apply.

	Home	University
Email	□	□
Facebook	□	□
Twitter	□	□
Wikis	□	□
Skype	□	□
Other	□	□

Please specify _____

2-Which activities are you doing with the tools you checked in Q1 as part of your **learning activities**? Tick all that apply.

Please specify_____

Chatting/Discussion	□
Assignment submission	□
Quizzes	□
Document sharing	□
Video conferencing	□
Other	□

3-On average, how many hours a day do you use the tools in Q1 **for learning activities**? Check one box only for each tool.

	I do not use it	Less than 1hr	Greater than or equal to 1 hr but less than 2 hrs	Greater than 2 hrs
Email	□	□	□	□
Facebook	□	□	□	□
Twitter	□	□	□	□
Wikis	□	□	□	□
Skype	□	□	□	□
Other	□	□	□	□

Please specify_____

Section III:Trust

4- Express your personal feelings while you are using those tools for learning activities. Tick all that apply.

	Ease of use	Afraid	Worried	Pleased	Motivated
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

5-How secure do you think those tools are? Check one box only on each row.

Secure means that information shared by the tool will only be accessible to those for whom it is intended.

	Very secure	Secure	Neither secure nor unsecure	Unsecure	Not secure at all
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

6. How safe to use do you think those tools are? Check one box only on each row.

Safe to use means the tool is protected from harm such as viruses, spyware, etc..

	Very safe	Safe	Neither safe nor unsafe	Unsafe	Not at all safe
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

7- How much privacy do you think these tools offer when being used for **learning activities**? Check one box only on each row.

Privacy: the ability of an individual or group to isolate information about themselves and thereby reveal themselves selectively.

	Has strong privacy	Has privacy	Neutral	Has little privacy	Has no privacy at all
Email	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Wikis	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

Please specify_____

8- Would you like to use OCG tools in future **for learning activities** and why? Explain your answer.

Yes ☐ No ☐

_____

_____

Section IV: Motivation

The following questions concern your experience with the **learning activities** you did during your course work. For each of the following statements, please indicate how true it is for you, using the following scale:

1	2	3	4	5
not true at all		somewhat true		very true

1.	I think I was pretty good at this activity.	1	2	3	4	5
2.	I believe this activity could be of some value to me.	1	2	3	4	5
3.	I would describe this activity as very interesting.	1	2	3	4	5
4.	I think doing this activity could help me to achieve my goal during the course work.	1	2	3	4	5
5.	I thought this was a boring activity.	1	2	3	4	5
6.	I thought this activity was quite enjoyable.	1	2	3	4	5
7.	After working at this activity for a while, I felt pretty competent at it.	1	2	3	4	5
8.	I am satisfied with my performance on this activity.	1	2	3	4	5
9.	This was an activity that I couldn't do very well.	1	2	3	4	5
10.	I tried very hard using the tools provided.	1	2	3	4	5
11.	I didn't put much energy into the activity while using the tools.	1	2	3	4	5
12.	I was doing what I wanted to do while working on the activity.	1	2	3	4	5
13.	I was doing this activity only because the teacher wanted me to.	1	2	3	4	5
14.	I would be willing to do this activity again because it is useful.	1	2	3	4	5

<<<<End of the questionnaire>>>>

Questionnaire-3

University of Warwick
Computer Science Department
Secure email awareness
Questionnaire-3

Section I: Personal information

University: _____

University ID: _____

1. Age: ☐ Under 21 ☐ 22-25 ☐ 26 or more ☐ Prefer not to say

2. Course: ☐ CS ☐ CSYS ☐ CMS ☐ CBS ☐ DM ☐MSc ☐PhD
☐ Other: _____

3. Year of study: ☐ 1st ☐ 2nd ☐ 3rd ☐ 4th

4. Nationality: _____

It would be very helpful if I might approach you at later point to speak to you about your experiences…
If you are comfortable for us to do that, please leave your email address: _____

If you have any enquiries, please email me at : r.aladraj@warwick.ac.uk

Section II: Email usage

5. Which webmail service/s do you use to read your email? Check all that apply.

☐ Gmail
☐ Hotmail
☐ Yahoo
☐ Other …..Please indicate _____

6. **Which computer application/s do you use to read your email? Check all that apply.**
☐ Apple Mail
☐ Thunderbird
☐ Microsoft Outlook
☐ None- I only use webmail
☐ Other ….Please indicate _____

7. Which of the email clients that you checked in Q5 and Q6 do you use most often?

_____

8. On average, how often do you access your email?

☐ More than 9 times/day
☐ 5 to 8 times/day
☐ 1 to 4 times/day
☐ A few times a week or less
☐ I never access my email

9. **Secure email** is a safe, efficient alternative to regular email, the user can feel confident that information shared by the email will only be accessible to those whom you have authorized to gain access.

A. There are various different views on the exact meaning of secure email. The following are some possible secure email meanings. Please tick all that you think apply

Secure email

a. Supports encrypted information that can be read by your intended recipient. ☐

b. Is authorised with digital signature. ☐

c. Detects spoofing or phishing. ☐

d. Hasn't been corrupted during transmission. ☐

e. If it has attachments, the attachments will have been scanned by anti-virus software. ☐

f. Has been filtered through anti-spam detectors. ☐

g. Other ☐

Please specify: _____

B. Based on the categories in part A, please tick each of those categories which you think your usual email client (your answer to Q 7) addresses:

a. Supports encrypted information that can be read by your intended recipient. ☐

b. Is authorised with digital signature. ☐

c. Detects spoofing or phishing. ☐

d. Hasn't been corrupted during transmission. ☐

e. If it has attachments, the attachments will have been scanned by anti-virus software. ☐

f. Has been filtered through anti-spam detectors. ☐

g. Other ☐

Please specify: _____

C. Based on the previous information about secure email in Q 9, how secure do you feel with your usual email client (your answer to Q 7)? Please check only one box:

Very Secure	**Secure**	**Neither secure nor insecure**	**insecure**	**Very insecure**
☐	☐	☐	☐	☐

Section III: Secure email awareness

10. This checklist is to find out your awareness of secure email. Read each sentence and indicate how often that statement relates to your use of email.

Statements	Always	Most of the time	Sometimes	Occasionally	Never	I don't understand what you mean
a. I send email that is digitally signed	☐	☐	☐	☐	☐	☐
b. I send email that is encrypted	☐	☐	☐	☐	☐	☐

Please comment on your previous two responses: (optional) _____

11. When I send email unsigned or unencrypted, it is because (Tick all that apply):

	Signed email	Encrypted email
a. It is too hard to do	☐	☐
b. I am worried that the recipient won't be able to read	☐	☐
c. I don't care enough to	☐	☐
d. I don't know how to	☐	☐
e. Other	☐	☐

Please specify: _____

12. For each of the following actions , check one box only to indicate how often you perform that action.

Actions	Always	Most of the Most of time	Sometimes	Occasionally	Never
a. I open unknown or unexpected email attachments.	☐	☐	☐	☐	☐
b. I send confidential information via email.	☐	☐	☐	☐	☐
c. I reply to unsolicited email messages (SPAM).	☐	☐	☐	☐	☐
d. I click on pop-ups in email or ads.	☐	☐	☐	☐	☐
e. I respond positively to those emails containing personally identifiable financial information.	☐	☐	☐	☐	☐
f. I click on embedded web links in email.	☐	☐	☐	☐	☐

13. For each of the following actions with <u>families/friends</u>, check one box only to indicate how often you perform that action.

Actions	Always	Most of the time	Sometimes	Occasionally	Never
a. I open unknown or unexpected email attachments.	☐	☐	☐	☐	☐
b. I send confidential information via email.	☐	☐	☐	☐	☐
c. I reply to unsolicited email messages (SPAM).	☐	☐	☐	☐	☐
d. I click on pop-ups in email or ads.	☐	☐	☐	☐	☐
e. I respond positively to those emails containing personally identifiable financial information.	☐	☐	☐	☐	☐
f. I click on embedded web links in email.	☐	☐	☐	☐	☐

a. I open unknown or unexpected email attachments.	☐	☐	☐	☐	☐
b. I send confidential information via email.	☐	☐	☐	☐	☐
c. I reply to unsolicited email messages (SPAM).	☐	☐	☐	☐	☐
d. I click on pop-ups in email or ads.	☐	☐	☐	☐	☐
e. I respond positively to those emails containing personally identifiable financial information.	☐	☐	☐	☐	☐
f. I click on embedded web links in email	☐	☐	☐	☐	☐

Activities	**Extremely important**	**Moderately important**	**Somewhat important**	**Slightly important**	**Not at all important**
a. Encrypting.	☐	☐	☐	☐	☐
b. Signing.	☐	☐	☐	☐	☐
c. Changing my password from time to time.	☐	☐	☐	☐	☐
d. Keeping updated installed Spam and Anti-Virus protection software.	☐	☐	☐	☐	☐

14. For each of the following actions with <u>a powerful member of an institution/organization</u> , check one box only to indicate how often you perform that action.

Questionnaire-4

University of Warwick
Computer Science Department
Questionnaire no.4
Resala Aladraj, PhD candidate

Date: _____

Form no. _____

I am a PhD student and I am interested in security issues in collaborative groupware tool usage. The purpose of this activity is to explore student perceptions of Online Collaborative Groupware (OCG) tool usage and their motivation towards secure usage. The data I receive will be kept confidential and will be stored anonymised. The data will only be seen by myself and my supervisor, Dr. Mike Joy. The Department's ethical procedures have been followed, and ethical consent has been granted for this questionnaire.

Personal information

1. Age: _____
2. Year of study: □1st □2nd □3rd □4th
3. Course code: _____

2- Email usage

Which of the following Email you used during the experiment? **You can tick on more than one option that applies to you.**

Yahoo ☐

Gmail ☐

Hotmail ☐

Other ☐

Please specify _____

3- Secure email is a safe, efficient alternative to regular email, the user can feel confident that information shared by the email will only be accessible to those whom you have authorized to gain access.

Please give us your opinion about how your frequent email was secure **while you were using it in the experiment** by clicking on the appropriate boxes below:

My email:	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
1. Enabled **two-step verification** when needed by SMS**.**	☐	☐	☐	☐	☐
2. Was authorised with signature.	☐	☐	☐	☐	☐
3. Enabled filtering of junk emails and phishing.	☐	☐	☐	☐	☐
4. Had not been corrupted during transmission.	☐	☐	☐	☐	☐
5. If it had attachments, the attachments had been scanned by anti-virus software.	☐	☐	☐	☐	☐
6. Connected over a secured network by setting the browser connection to "**Always use HTTPS**."	☐	☐	☐	☐	☐
7. Recovered the passwords by "**Change password recovery options**".	☐	☐	☐	☐	☐
8. Allowed me to use a code instead of password by using "**Get a single use code to sign in with"**	☐	☐	☐	☐	☐

4- Actual Email usage

How often did you use email **during the experiment**?

Never ☐ Rarely ☐ Occasionally ☐ Often ☐

5- Trust *(Adapted from McKnight et al 2002)*

Express your personal feelings **while you were using email in the experiment after setting the security.**

During the experiment:	Strongly agree	Agree	Undecided	Disagree	Strongly disagree
1. I felt pleased when I accessed the email.	☐	☐	☐	☐	☐
2. I felt motivated when I accessed the email.	☐	☐	☐	☐	☐
3. I relied (trusted) on the email after setting the security.	☐	☐	☐	☐	☐
4. I believe the email is dependable.	☐	☐	☐	☐	☐
5. I was totally comfortable accessing the email.	☐	☐	☐	☐	☐
6. I always felt confident that the right things would happen when I was using the email.	☐	☐	☐	☐	☐
7. I think now that email will enable me to do what I need to do.	☐	☐	☐	☐	☐
8. I felt very good about how things went when I was using the email.	☐	☐	☐	☐	☐

6- Perceived Usefulness (*Adapted from (Hubona & Burton-Jones, 2003))*

Please give us your opinion about how your email was useful **while you were using it in the experiment** *by clicking on the appropriate boxes below:*

The email I used in the experiment:	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
1. Enabled me to accomplish tasks more quickly.	☐	☐	☐	☐	☐
2. Improved my assignment performance.	☐	☐	☐	☐	☐
3. Increased my productivity.	☐	☐	☐	☐	☐
4. Enhanced my learning effectiveness.	☐	☐	☐	☐	☐
5. Made it easier for me to study.	☐	☐	☐	☐	☐
6. Was useful in my job.	☐	☐	☐	☐	☐

7- Perceived Ease of Use (*Adapted from (Hubona & Burton-Jones, 2003) et al 1986)Please give us your opinion about how your frequent email was easy to use* **while you were using it in the experiment** *by clicking on the appropriate boxes below:*

During the experiment:	**Strongly agree**	**Agree**	**Undecided**	**Disagree**	**Strongly disagree**
1. The email was easy for me to access.	☐	☐	☐	☐	☐
2. It was easy to get emails to do what I wanted them to do.	☐	☐	☐	☐	☐
3. My interaction with email was clear and understandable.	☐	☐	☐	☐	☐
4. It was easy to become skilful using email.	☐	☐	☐	☐	☐
5. It was easy to remember how to perform tasks using email.	☐	☐	☐	☐	☐

Appendix B

Interviews

Security Issues and collaborative groupware
In Web-Based E-Learning Systems
Interviews-1

Name of the interviewee:
Date:
Venue:
Duration:

2) Introduction about my interviews

For example: to explore the student's perception of the security that relates to the different collaborative tools.
Would mind recording the interview

3) Warm-up period:

- What are you study?
- How usually are you study?
- Have you ever used communication tools in your study like facebook
- Have you heard about Collaborative groupware learning tools?
- What are these?

4) Cool-up period:

- What are the problems have you faced during you conducting theses tools?
- Have you faced security problems ?what are these?
- What are your suggestions to solve such of these problems?
- Would you like to continue using these tools in your learning?why?

AppendixC

SWGG security settings

University of Warwick
Computer science department
PhD Research case study 2
Resala AlAdraj

How to secure Gmail

1-Enable two-step verification: To address the issue phishing, scam or when you accidentally expose your password, Google now offers two-step verification, in which Google will send you an SMS with a special code that you enter as the second part of the log-in process.

2: Be a password strategist: When choosing a password, there are two things you should be doing. First, choose a password that is unique to your Gmail account-don't use it for any other service. Once you've chosen a password, head to Password Meter to check its strength.

3: Enable HTTPS security: If you access Gmail over an unsecured network as at a cafe, library, or shop--you instantly become vulnerable to hackers. Make sure you're browsing public Wi-Fi safely, and that you're using Gmail with HTTPS security. To enable HTTPS, sign in to Gmail and go to Mail settings (upper right) > General. Set "Browser Connection" to "Always use HTTPS."

4: Update your backups: Sign in to Gmail and head to Account settings (upper right) > Accounts and Import > Change password recovery options. Here, you can add an e-mail address, a phone number, and a security question you can use to recover your account if a hacker changes your password.

5: Check account activity: It could be that a hacker is accessing your account without your knowledge. To check, sign in to your Gmail account and go to the bottom of the page. You'll see a line that says "Last account activity..." At the end of this line, click "Details" and you'll see when, how, and where your account is being used. If you suspect any un kosher activity, immediately change your password and security questions, and enable two-step verification

Mail spam is one of the greatest annoyances of our time.

For the third and fourth quarter of 2008, the Messaging Anti-Abuse Working Group reported that approximately 90% of all eMail was spam. That's an incredible number. It clearly demonstrates how much time and energy must be wasted to receive, identify and get rid of spam.

While spam protection has become quite effective at recognizing unsolicited bulk eMail, it's still impossible to filter out and stop receiving spam.
Besides regular spam, we receive a lot of advertising in our inboxes. Although these eMails are often personalized, they still classify as spam. However, these eMails were usually created based on information we made available about ourselves, rather than straight forward eMail guessing.
Hence, one way to help stop receiving spam is to control the information you're releasing about yourself. The best way to do this is to protect and hide your eMail address.

1. Scramble your eMail address

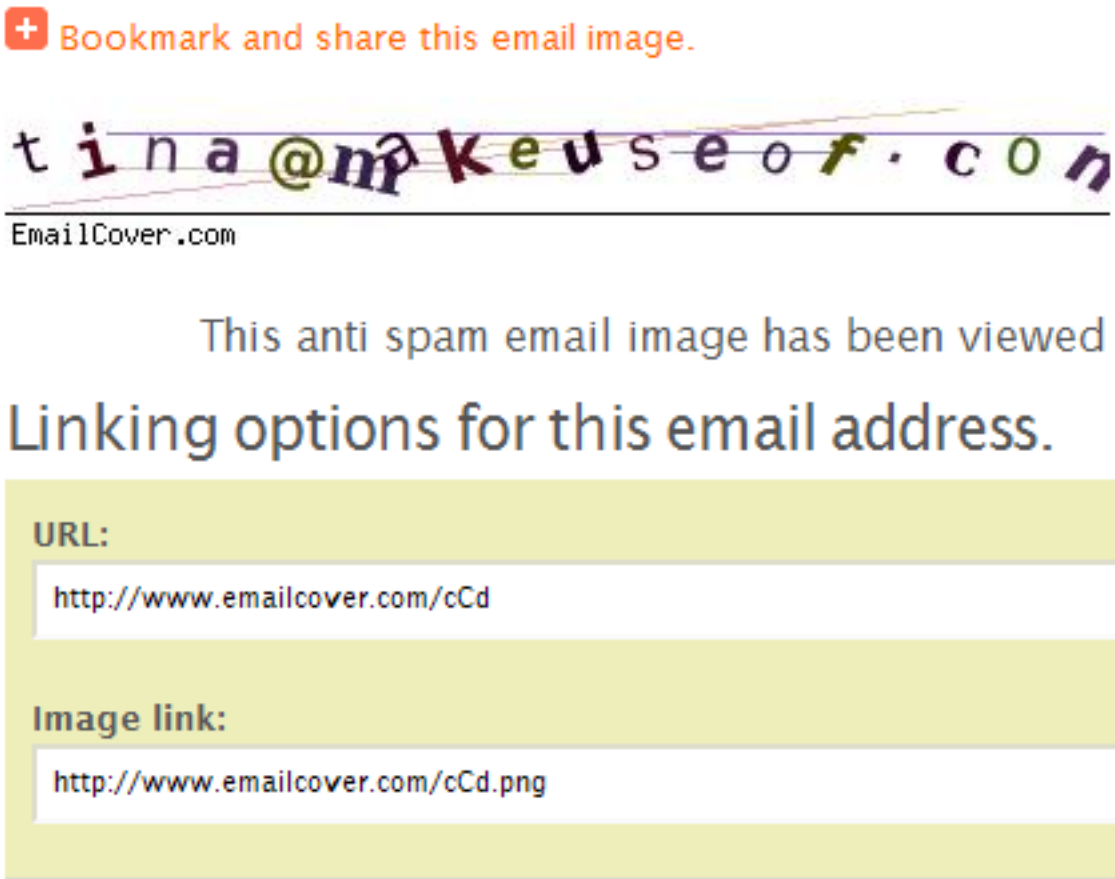
We often have to share our eMail address online. So what can be done to make it difficult for a bot to simply copy the information?
Rather than publishing your eMail address in its standard format, you could scramble

and thereby conceal it. It requires an attentive and intelligent mind to recognize a scrambled eMail address and re-assemble it into a functional format.
A scrambled eMail address can look something like this: *tina at make use of dot com*

And this is the unscrambled eMail address: tina@makeuseof.com

2. Hide your eMail address in an image

A similar solution is to hide the eMail address within an image. There are several tools that will do this for you. One which provides many other functions is ~~EmailCover~~.
Not only does it produce an image containing your eMail address in a CAPTCHA format, it also hosts the image and provides you with a set of links you can use to embed the image in your website, signature or on social network sites. Using the bookmark feature you can directly share your eMail address with the most popular sites. Finally, the tool records how often the image has been viewed.

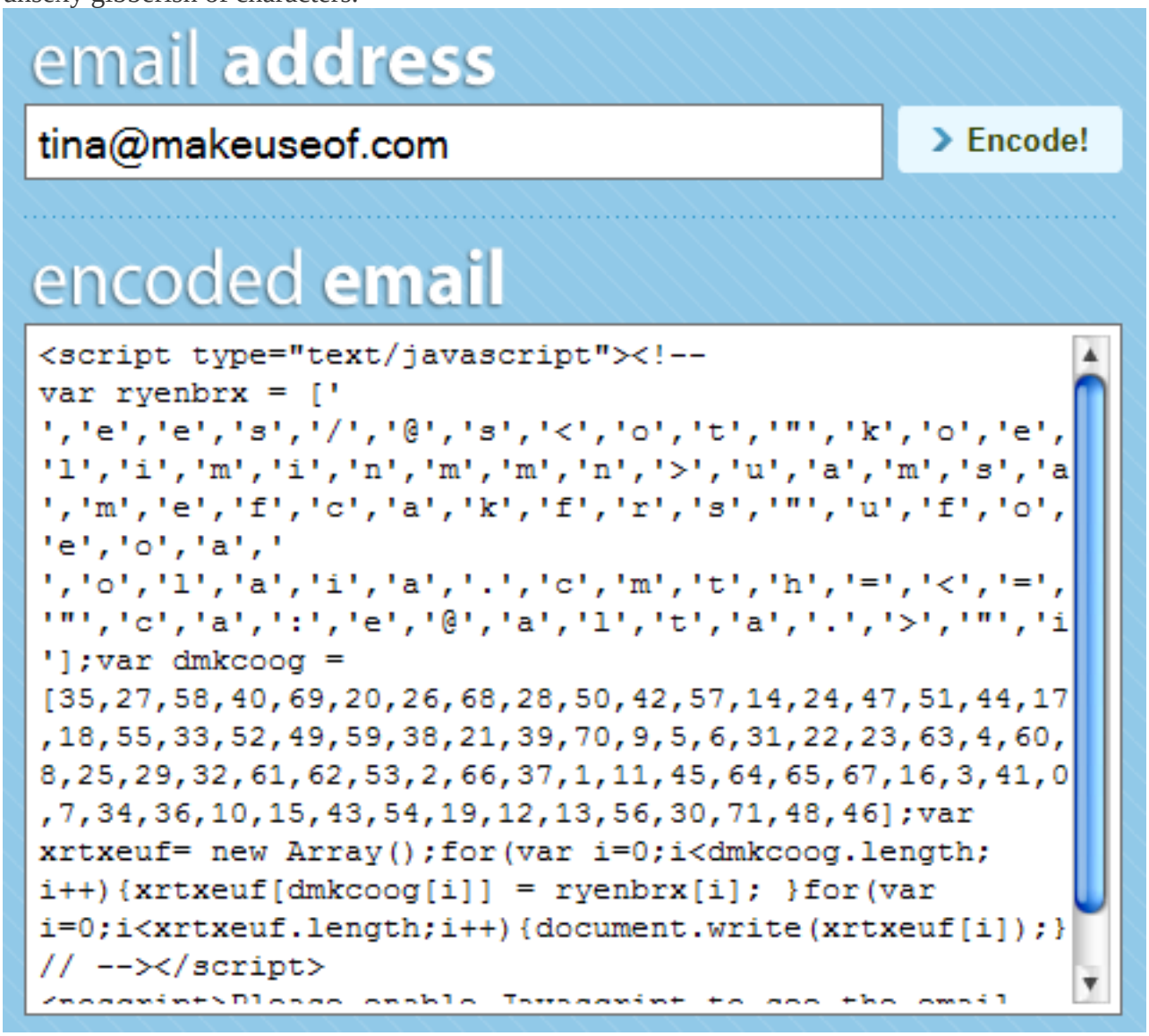


Similar tool: E-Mail Icon Generator.

If you want to be sure only the smartest people can guess your eMail address, combine 1 and 2.

3. Encode your eMail address

If you *must* post an active eMail link, for example to give people a quick and easy way to contact you, you can encode your eMail address in a way that is not readable by spambots, which extracts eMail addresses from websites.
MailTO Encoder will decode your eMail address using Javascript. The result is a rather unsexy gibberish of characters.

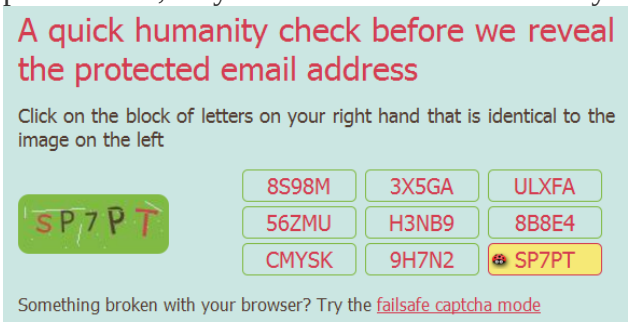


Similar tools: E-mail Anti-SPAM Encoder (no Javascript), Hivelogic Enkoder

4. Hide eMail behind a test

With a tool called scr.im, you can protect your eMail address by hiding it behind a

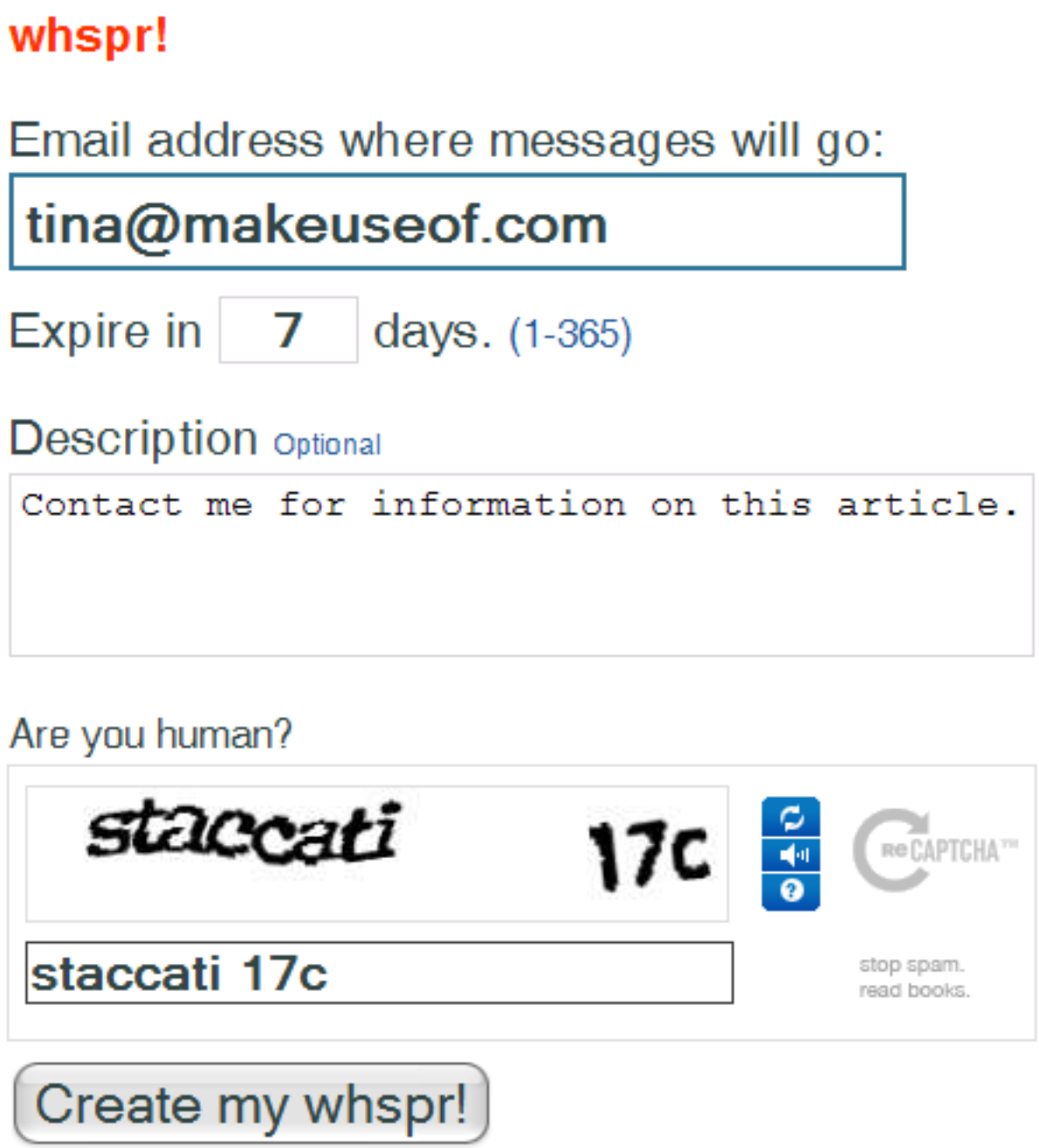
simple test.
At scr.im's start page you enter your eMail address and the site will provide you with an ultra short scrimmed URL, along with custom HTML to share your eMail address on Twitter, Facebook, within HTML documents and in forums.
The link will lead anyone needing your eMail address to a quick test. If they manage to pass the test, they will be rewarded with a fully active link to your eMail address.



Similar tool: [NO LONGER WORKS] reCAPTCHA, [NO LONGER WORKS] tinymail.me

5. Don't share your eMail address

The last resort is to not share your eMail address at all. Set up temporary inboxes or forms through which you can be contacted indirectly.
For example whspr! allows you to create a temporary form, which will relay messages to your eMail address. Users have to prove they are human by passing a CAPTCHA test.

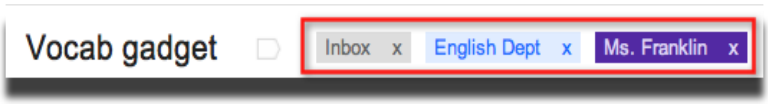


Similar tools: ~~kontactr~~, contactify

Gmail Apps Mail

Sidebar links	Description
COMPOSE	**Compose Mail** opens a new message window
Inbox (26)	**Inbox** shows your conversations (the number in parentheses indicates how many unread conv you have).
Starred	**Starred** shows you only messages you've marked with a star (use stars to mean whatever you
Important	**Important** shows messages
Chats	**Chats** lists your archived Chat conversations.
Sent Mail	**Sent Mail** shows messages you've sent
Drafts (9)	**Drafts** houses messages you've started and saved to work on later
Spam (1)	**Spam** is where we send the messages we think are suspicious
Trash	**Trash** is where messages you delete end up; you can empty the trash whenever you feel like it

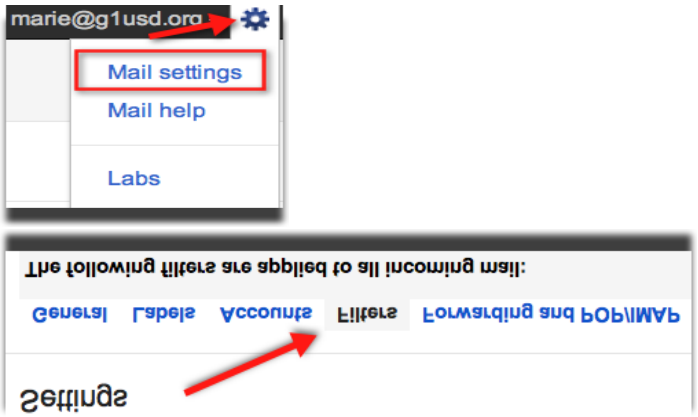
1. Labels
While you won't find folders in Apps Mail, you can use labels to organize email messages. Because multiple labels can be applied to the same conversation, you have the flexibility to manage conversations that may fall under more than one category.



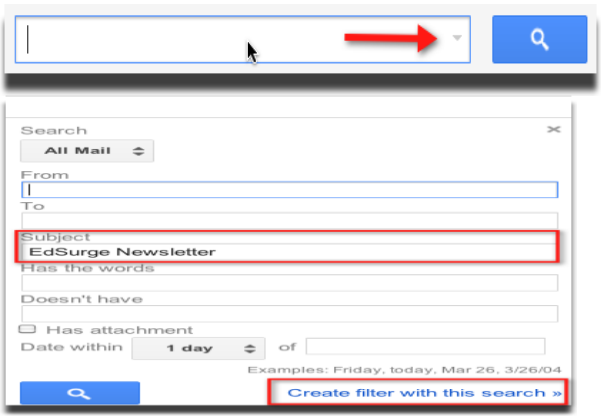
By clicking on a label, you can view a chronological list of all conversations that have been tagged with that particular label. Unlike folders, messages with multiple labels will display in each label.

2. Filters
Create filters that automatically label, archive, delete, and forward messages and let Apps Mail do the work for you. You can control which actions are taken based on the message subject, who sent the message, what text is included, whether it has an attachment, etc.

To get started with filters, click the Settings link in your account and select the Filters tab

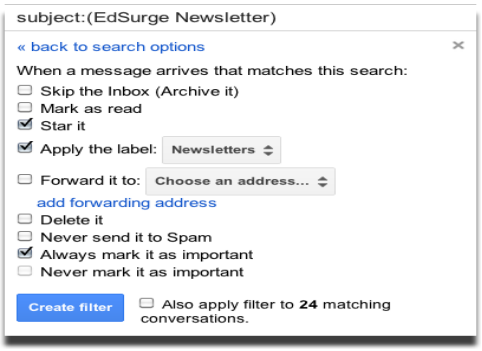


or click on the drop-down arrow in the search box, enter in any criteria, and then select **Create filter with this search**



A new dialog box will open and you will be able to apply additional parameters for your filter. Make sure you click

Create Filter



Signatures

You can set a default signature that will be applied to all sent messages. To set up your signature, visit the Settings under the General tab.

Rich text signatures are available in Apps Mail allowing you to add your own formatting, images and links to your email signatures. If you have configured your Gmail account to also send mail using the Send mail as/custom 'from' feature, then you can now also have a unique signature for each these other addresses that you've added to your account.

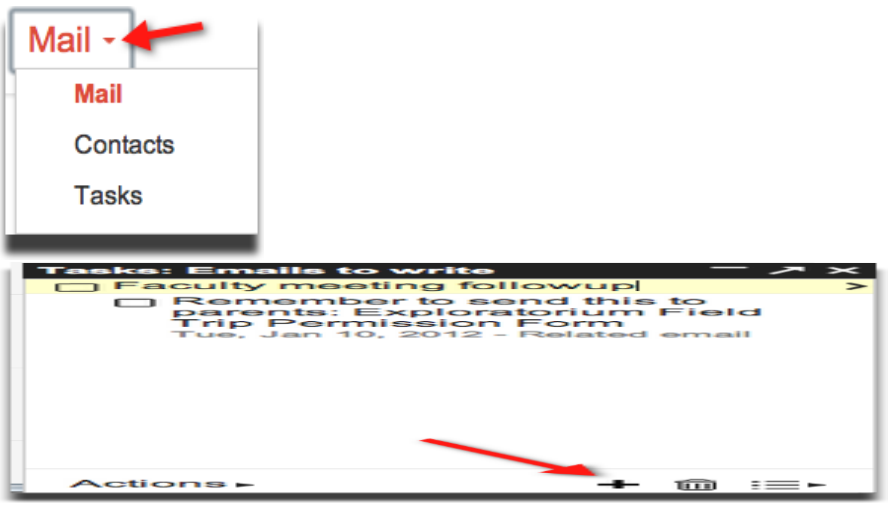
Starred items

In Apps Mail, you can mark priority messages just as you can add a red flag in Outlook. Simply click the star icon (next to the sender's name) to star a message (click it again to remove the star). To see all the messages that you've starred, click the Starred link on the left side of your account.

Email notification To have email notifications pop up in the corner of your screen when you receive a new message, you can download the Google Talk client (Windows only) or the Gmail Notifier (Windows & Mac).

Tasks

Google Apps Mail also allows you to keep track of to-do lists in a similar way to Outlook's tasks feature. The 'Tasks' link appears on the left side of your account by clicking the drop-down arrow next to the mail link. Click on 'Tasks' to open the to-do list window. In the tasks window, click the '+' icon to get started and add a task. Once you've completed a task, check it off the list.



If you no longer want to grant somebody else access to your account, follow these instructions:

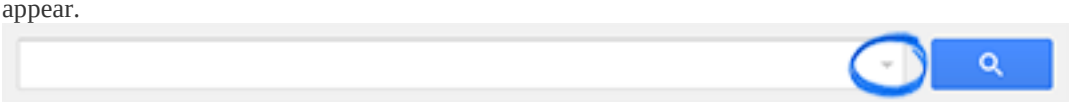
. Click the **gear icon** in the top right corner of Gmail and choose **Mail settings**
. Click the **Accounts and Import** tab.
. In the "Grant access to your account" section, click **delete** on any account you want to remove.

Using filters

Gmail's filters allow you to manage the flow of incoming messages. Using filters, you can automatically label, archive, delete, star, or forward your mail, even keep it out of Spam.

To create a filter

. Open Gmail.
. Click the down arrow in your search box. A window that allows you to specify your search criteria will appear.



. Enter your search criteria. If you want to check that your search worked correctly, click the search button.
. Click **Create filter with this search** at the bottom of the search window. If you need to verify the search results, you can click the **x** to collapse the filter options. Clicking the down arrow again will bring the window back with the same search criteria you entered.
. Choose the action(s) you want the filter to take. To keep organized, many people like to have incoming messages automatically labeled and removed from their inbox until they can look at them later at a more convenient time. If you want to do this, make sure to select **Skip the Inbox (Archive it)** and **Apply the label:** when you create your filter.
. Click the **Create filter** button.

Please note: When you create a filter to forward messages, only new messages will be affected. Any existing messages that the filter applies to will not be forwarded.

To use a particular message to create a filter

Open Gmail.
Select the message in your message list.
Click the **More** button, then **Filter messages like these**.
Enter your filter criteria in the appropriate field(s).

To edit or delete existing filters

Open Gmail.
Click the gear in the top right.

Select **Settings**.
Click the **Filters** tab.
Find the filter you'd like to change and click **edit** or **delete** to remove the filter.
If you're editing the filter, enter the updated criteria for the filter in the appropriate fields, and click **Continue**.
Update any actions and click the **Update filter** button.

You can create an unlimited number of filters, but only 20 filters can forward to other addresses. You can maximize your filtered forwarding by combining filters that send to the same address.

To export or import filters

If you're a filter pro and have a great filter system that you want to use in another account or share with a friend, you can export and import filters.

Open Gmail.

Click the gear in the top right. 

Select **Settings**.

Click the **Filters** tab.

To export a filter, check the box next to the filter, and click the **Export** button at the bottom of the page. This will give you a .xml file, which you can edit in a text editor if you'd like.

To import a filter, click the **Import filters** link at the bottom of the page. Choose the file with the filter you'd like to import and click the **Open file** button. Click the **Create filters** to finish importing the filter.

. Select *Options* | *More options*... (or just *Options* in Windows Live Hotmail classic) from the toolbar.
. Follow the *Automatically sort e-mail into folders* link under *Customize your mail*.
. Click *New filter*.
. Select the desired filtering criterion under *Which messages are you looking for?*.
. Choose the folder to receive all mail matching your criterion under *Where do you want to put these messages?*.

Click *Save*.

4 Best Practices To Secure Your Hotmail Account

1. Using strong passwords

This is the first and foremost setting that a user needs to be responsible for. You should be using strong and secure passwords so that no one will be able to use brute force methods to guess your password. So what is a strong or secure password? The password which is:

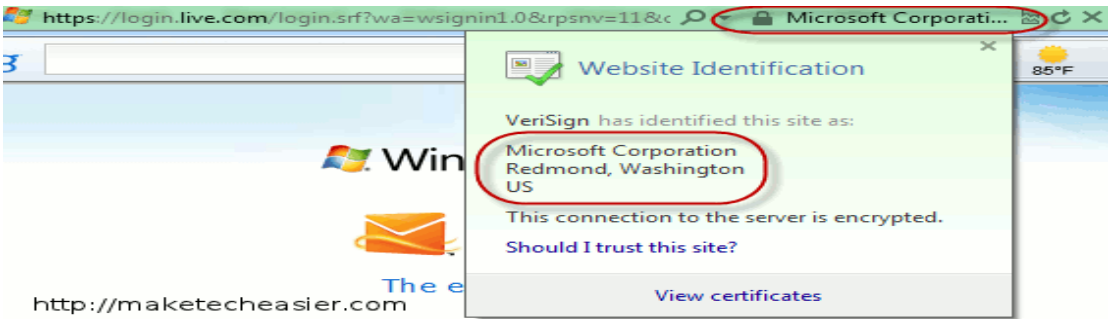
Not a dictionary word (regardless of any language)
Not a variation of a dictionary word
Not a sequential or repeated word
Doesn't include any personal information like name, birthdate, Govt. issued IDs etc.

There are many random password generators but if you want to remember your password then you should follow the way to create passwords recommended by Microsoft itself.

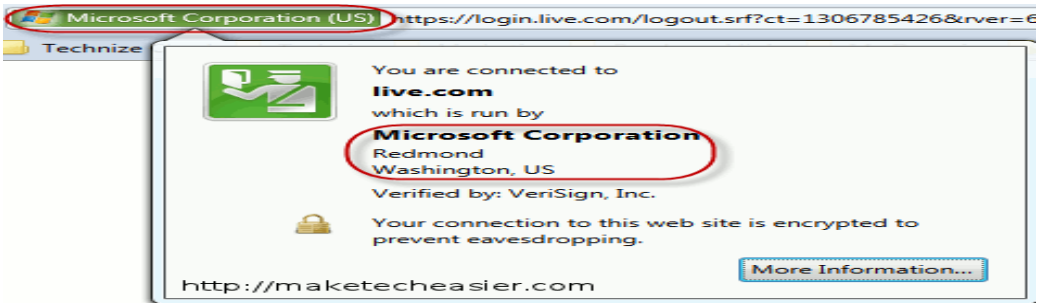
2. Connecting With HTTPS

Using HTTPS instead of HTTP means that you're using a secure means of communication between the Hotmail servers and your computer. If a hacker intercepts the connection during the communication, the connection will simply break and the hacker will not be able to get any information about the communication. Almost all the modern browsers will display a green bar that shows the owner of the site in the address bar. Make sure that the owner of Hotmail.com when you open it is Microsoft Corporation.

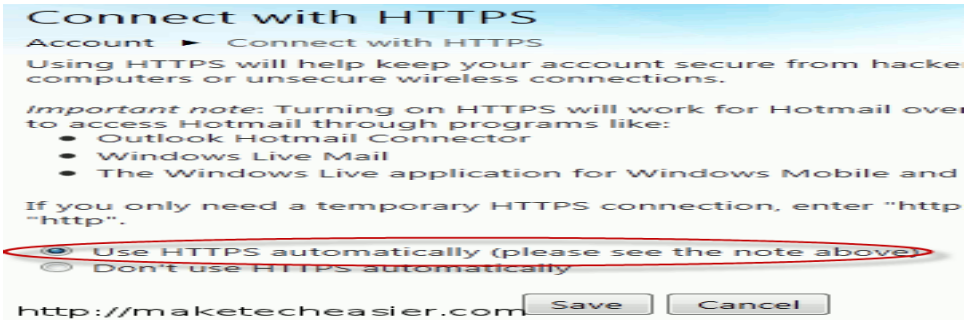
Here's how it looks like in Internet Explorer:



And here's the screenshot from Firefox:



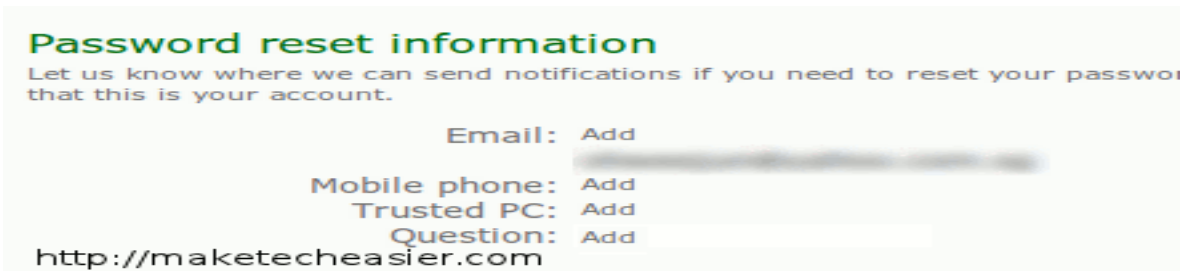
To always use HTTPS, just go to the Microsoft manage SSL page and select "*Use HTTPS automatically*".



Please note that if you're using a desktop client with Outlook Hotmail Connector or Windows Mobile, you'll get some problems with HTTPS. Then you can leave the above settings to "Don't use HTTPS automatically" and then always open Hotmail using *https://www.hotmail.com* in order to check your email.

3. Password Reset Information

You must ensure that your password reset information in your Hotmail account is always up to date so in any case if you forget your password, you'll always be able to reset your password using the recovery information. To reset your password information, you'll need to go to Windows Live account page.



You should always have a secondary email address that you can attach to your Hotmail account so that your password reset information is sent to your secondary account if you forget the password.

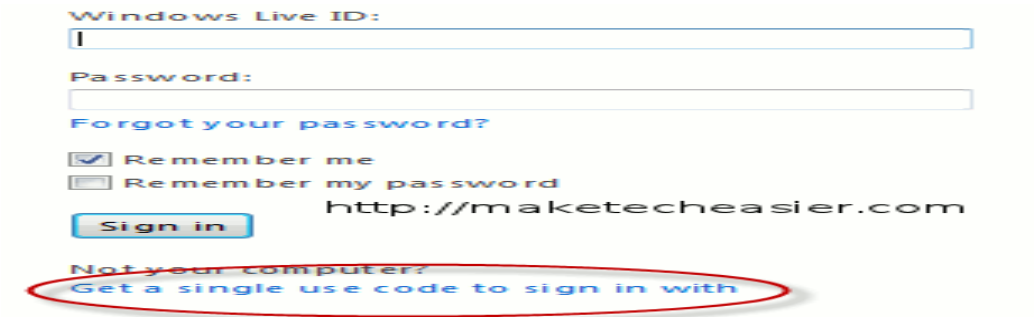
You can also add your mobile number as a recovery option so that the password reset information can be sent to your mobile phone in case of emergency but this option is only available to a few selected countries right now.

You can also add a Trusted PC if you use your account only on one PC. Windows Live Essentials is

needed to be installed in order for this feature to work.

And the last and most important is the security question. The security question is like a password. You should always specify a secure security answer in order to have your account secured and away from hackers. Please refer to the "using strong passwords" topic for more information about secure passwords.

4. Using Hotmail On A Public Computer



There are times when you'll need to check your email on a public computer when your own trusted computer is not available. You should always use HTTPS instead of simple HTTP on public computers. There is another feature "Get a single use code to sign in with" which works great if you are residing in a supported country. You can get a code for one time use on your mobile when you want to sign in to your Hotmail account on a public computer. This will ensure that you don't have to type your real password and will use an auto generated password which will work only one time.

Keeping all these points in mind when using your Hotmail account will make sure that your account will always remain safe from wrong hands and hackers.

How to secure Skype

Instructions

Privacy Settings

1. Open Skype and click "Tools" on the Main menu bar. Click "Options" to open the Options menu.
2. Click "Advanced." Check the box next to "Automatically Download and Install It" under the New Versions of Skype section. This will keep your version of Skype updated and help protect against known security threats by letting the program automatically download new security patches.

3. Click "Privacy Settings" and select "Allow Only People on My Contact List to Contact Me." This will keep your Skype account private and prevent unknown people from contacting you and attempting to set-up a connection.
4. Click "Save" to save your account settings.

Account Settings

5. Open a Web browser and navigate to the Skype homepage (please See Resource section for a link to the Skype homepage.)□□
6. Click "Account." Type in your Skype name and password. Click "Sign Me In."
7. Select "Change Your Password."
8. Type in a new password and retype it to confirm. Click "Save."

Tips & Warnings

1. Always check any files that have been sent to you through Skype with your antivirus software before opening them. Right-click on the file and select your antivirus scanning option.
2. Never tell anyone your Skype password and don't click on any emails asking for your Skype account information. Skype never requests account information via email and only conducts business through its website.

Make Your Facebook Account Private

Head to your privacy settings under the Account menu at the upper right corner of your Facebook page.

On the privacy settings page, you'll See five categories: Profile, Contact Information, Applications and Websites, Search and Block List.

Start at the top with Profile information and change all the options to "Friends." This will stop people you don't know from accessing any of your personal data.

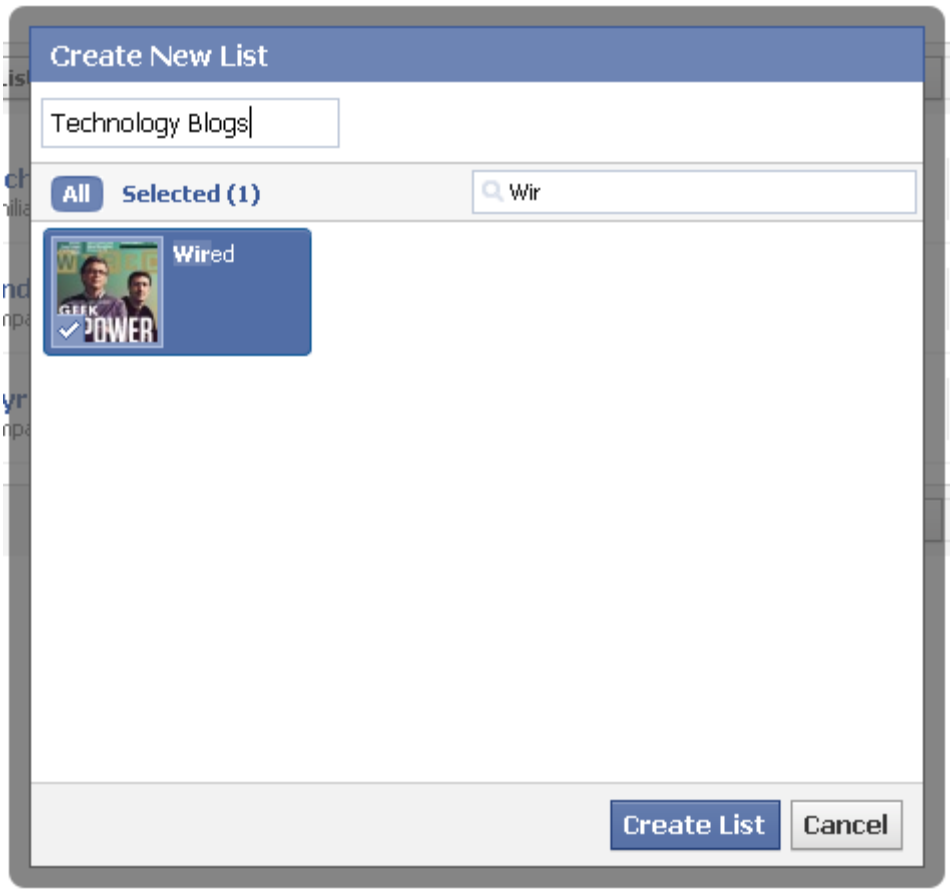
Do the same for your contact information, most of which, thankfully, still defaults to Only Friends.

Also be aware that each setting has a "customize" option which allows you to, for example, set your information to "visible only to friends" but also block certain "friends" (like your mom, so she won't See the drunken, late night rants you post on your Wall).

Using Friend Lists

A good practice is to group all your contacts in Facebook. To do that, you can use Friend Lists.

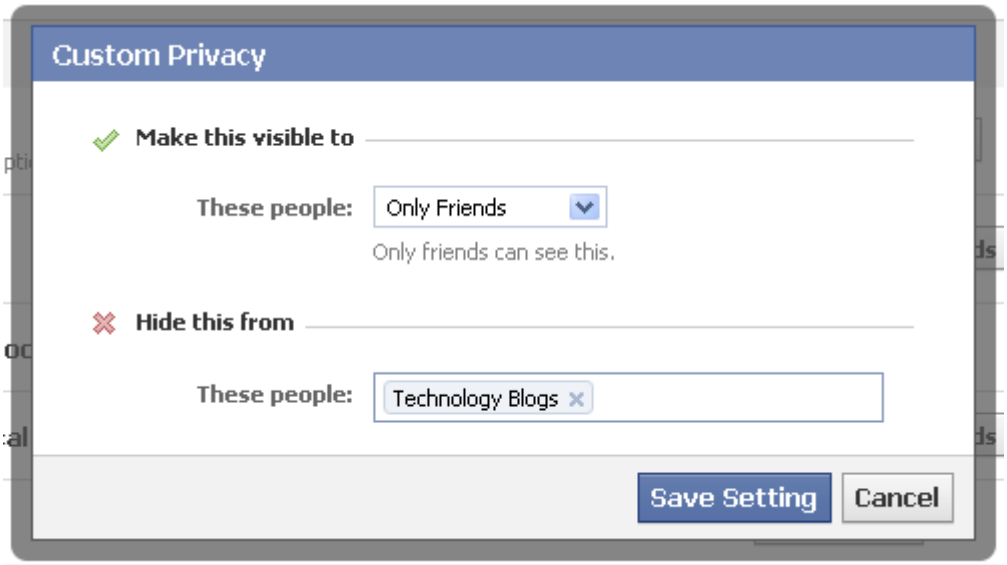
To create a Friend List, go to the Edit Friends option under the Account menu, then select the Friends option beneath the Lists group on the left side of the screen. In the new page select "Create New List" at the top to display a window where you can type a name for your new list and select which friends belong to it.



Creating a new Friend List in Facebook.

Besides creating obvious lists (such as Family, Good Friends, Classmates, etc.) it would be recommended that you create a *"Nothing to do with me"* list, so you can add people that doesn't have a close relation to you to this category.

Now you can go back to the Privacy Settings option and use the lists to make visible or hide anything in your profile to that group of people by using custom settings. And remember to use the "Nothing to do" list to hide the sensitive elements of your profile from strange eyes.



Customizing privacy setting by using a Friend List.

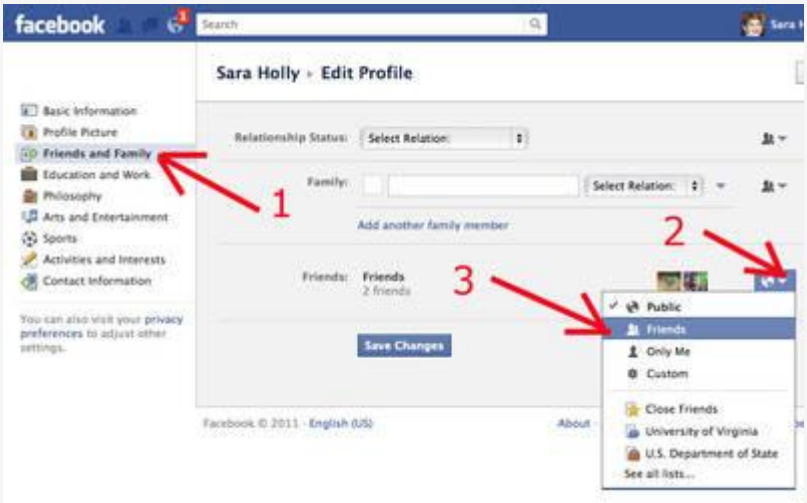
Take These Steps to Make Facebook Private

By Leslie Walker, About.com Guide

2 of 4

Previous Next

How to Take Your Facebook Friends List Private



Facebook makes your friends list public by default. That means everyone can See it, even if they are not your friend.

You can change that with just a few clicks. The easiest way is you to go to your profile page to edit the visibility of your friends list. Clicking your name at the top right of your Facebook home page always takes you to your profile page, then click the "Edit Profile" button at top right.

You should reach the page shown in the screen grab above. Follow the following three steps (each is marked in red above) to change the visibility of our friends list.

1. **Click "Friends and Family"** in the left sidebar (1) and a new menu will appear on the right, in the main body of the page.The "Friends" option in the middle of the page refers to your list of friends on Facebook.
2. **Click the down arrow next to the globe at left:** You control who can See your friends list by clicking on the audience selector drop-down menu (2), which by default is set to the globe icon for "Public."
3. **Change the default.** When you click the small down arrow, a longer list of options will appear (3). It includes "Friends," "Only Me," "Custom" and any additional networks or groups you've joined below that.It's a good idea to change the default setting for who can See your list of Facebook pals to "Friends," so only people you've friended on Facebook will have access to this list.

Next, let's look at how to control who Sees your Facebook profile (read this article if you're confused about the difference between your profile, home page, Wall and news feed.)

You should always stop and think about whether your profile and Timeline/Wall reveal too much information about you.

---

has more than 50 different e-mail settings for the main Facebook application alone, plus a setting for each of your add-on applications. Turn as many to â€˜Off' as you care to.

How to Hide Your Facebook Friends List

From Daniel Nations, former About.com Guide

The setting is located on your profile page. (Image of Facebook)

With the recent changes to Facebook's privacy settings came the decision to open up a user's friends list to anyone who visited their profile. After a hue and cry from Facebook users and advocacy groups, Facebook relented and provided a way to hide the friends list. Unfortunately, they didn't make it altogether easy to find out how to hide your Facebook friends list.

Don't bother looking in the privacy settings. For some reason, Facebook decided to bury the setting in the profile itself.

To hide your Facebook friends list, go to your profile page and locate the Friends box in the left column. There is a small icon of a pencil in the upper right-hand corner of the friends box that will open a small window containing the settings. Simply uncheck the box marked "Show my friends on my profile" and your friends list will no longer show up to visitors.

How to secure WikiSpace

Privacy and Permissions

Overview

Permissions let you define who can see, edit, and interact with your wiki or Private Label site.

Every Wikispaces wiki will let you set permissions at both the wiki and the page level, so access can be more restrictive at every level. For example, you can set your wiki to **Public**, but a single page to **Locked** — so anyone can see or edit most of the wiki, but only organizers can edit that one page.

You can also apply specific permissions settings to any file on your wikis, so you decide who can view, delete, and replace your files.

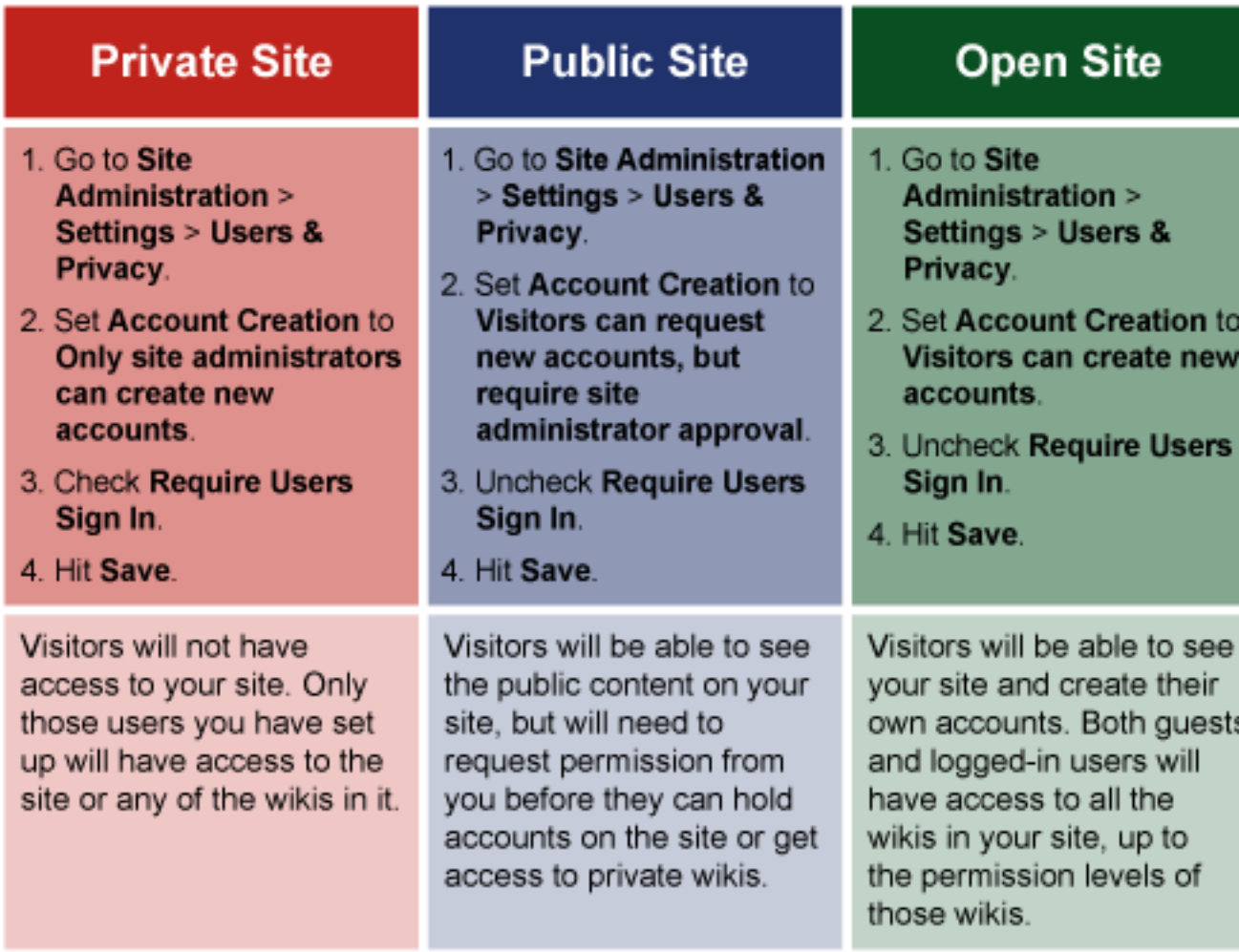
With Wikispaces Private Label, you have all those options, plus more robust privacy settings for your site as a whole.

Some subscription plans have more limited permissions options than others. Before you go on, take a minute to see what the options are for your plan:

Wikispaces Private Label

Because a Private Label site is a whole network of wikis, you have site-wide settings that are not available with a single wiki. Your Private Label site has its own user database, so you can choose how those users will interact with the site. You get to make decisions about whether they can rename their accounts or create new wikis, and you can turn the site's private messaging system on and off.

The two main privacy settings, however, are **Account Creation** and **Require Users Sign-in**. You can set these independently for a wide variety of site privacy levels. Here are the three most popular:



Private Site	Public Site	Open Site
1. Go to **Site Administration** > **Settings** > **Users & Privacy**. 2. Set **Account Creation** to **Only site administrators can create new accounts**. 3. Check **Require Users Sign In**. 4. Hit **Save**.	1. Go to **Site Administration** > **Settings** > **Users & Privacy**. 2. Set **Account Creation** to **Visitors can request new accounts, but require site administrator approval**. 3. Uncheck **Require Users Sign In**. 4. Hit **Save**.	1. Go to **Site Administration** > **Settings** > **Users & Privacy**. 2. Set **Account Creation** to **Visitors can create new accounts**. 3. Uncheck **Require Users Sign In**. 4. Hit **Save**.
Visitors will not have access to your site. Only those users you have set up will have access to the site or any of the wikis in it.	Visitors will be able to see the public content on your site, but will need to request permission from you before they can hold accounts on the site or get access to private wikis.	Visitors will be able to see your site and create their own accounts. Both guests and logged-in users will have access to all the wikis in your site, up to the permission levels of those wikis.

Popular Scenarios

Scenario 1

I have a Private Label site. I don't want it to be available to the public at all. Within my organization, there will be a few wikis that everyone will want to see, but most wikis should only be accessible to a few people — and that group will change from wiki to wiki.

1. Make sure that your users are members of the wikis that they ought to have access to, and not members of the wikis that they shouldn't have access to.
2. Go to **Site Administration** > **Settings** > **Users & Privacy**.
3. Check the box for **Require Users Sign In**, and hit **Save**.
4. For each individual wiki, go to **Settings** > **Permissions**.
5. For the wikis that everyone should have access to, set the wiki permissions to **Public**. For the wikis that only a few people should have access to, set the wiki permissions to **Private**. Hit **Update**.

Scenario 2

I have a Private Label site. My site is visible to the public, and I want the public to be able to view and edit most of the wikis on my site — and post to discussions.

. Go to **Site Administration** > **Settings** > **Users & Privacy**.
. Uncheck the box for **Require Users Sign In**, and hit **Save**.
. For each individual wiki, go to **Settings** > **Permissions**.
. Set the wiki permissions to **Public**, check the box for **Allow Message Posts from Non-members**, and hit **Update**.

Scenario 3

I have a single wiki, and I don't want my wiki to show up in a Google search.

1. Go to **Settings** > **Permissions**.
2. Set the wiki permissions to **Private**. *This option will not be available on Basic-plan wikis.*

Scenario 4

I have a single wiki. I've invited people to join, but I don't want them to be able to edit all of the pages in the wiki.

1. Go to the pages you don't want people to edit.
2. Click the More Page Options button and select **Lock** from the menu. *You can unlock the page later from the same menu.*

Scenario 5

I have a single wiki. I want to make it so that people don't have to sign in to see my wiki, but only people who join the wiki are able to edit it.

1. Go to **Settings** > **Permissions**.
2. Set the wiki permissions to **Protected**.

Scenario 6

I have a wiki for my classroom. I want to create pages that only certain students — or groups of students — can see or edit, so that my students feel secure in their work.

User-level settings are not available at this time, so there is no way to create user groups within a single wiki. We recommend creating multiple wikis and assigning your student groups membership to the different wikis.

1. Go to http://www.wikispaces.com/site/for/teachers to create a new K–12 Plus wiki for each student or student group.
2. Add the student or students as members of that wiki.
3. Go to **Settings** > **Permissions**.
4. Set the wiki permissions to **Private**.

Link: https://help.wikispaces.com/Privacy+and+Permissions

<h2>Javascript Required</h2> You need to enable Javascript in your browser to edit pages.

Appendix D

Experiments Assignments

Experiment's assignments

IT IS 101 Personal Productivity with IS Technology
Assignment #1
Chapter 2 &3
Due Date: 23rd Nov2012

1. What is the difference between pipelining and parallel processing? (5 Marks)

2. Define the term SOLID STATE and give three examples of SOLID STATE storage devices (5 Marks)

Please send your assignment by email to
gsulaibeekh@uob.edu.bh
in the email please write :
subject: ***ITIS101 Assignment #2***
in the email body
Student name
Student ID
Section

Assignment #2
Chapter 9
Due date: 10th Dec 2013

1. ***Define Salami Shaving and Data diddling***
2. ***What is Forgery, and cyber gangs?***
3. ***Define and explain the different between the two different types of phishing***
4. ***What is cyber gangs?***

Please send your assignment by email to
gsulaibeekh@uob.edu.bh
in the email please write :
subject: ***ITIS101 Assignment #3***
in the email body
Student name
Student ID
Section

Appendix E

SPSS Analysis

Chapter five

Reliability Statistics

Cronbach's Alpha	N of Items
.771	7

Item Statistics

	Mean	Std. Deviation	N
mot1	4.02	.976	44
mot2	4.20	.930	44
motv3	4.02	1.171	44
mot7	3.64	.990	44
mot8	3.93	.873	44
mot12	3.75	1.184	44
mot14	4.34	1.077	44

secondr_school

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ahd zahe	3	5.9	5.9	5.9
	ahmdomra	1	2.0	2.0	7.8
	alkifah	1	2.0	2.0	9.8
	almarifa	2	3.9	3.9	13.7
	alrawen	1	2.0	2.0	15.7
	alwaffa	1	2.0	2.0	17.6
	apg priv	1	2.0	2.0	19.6
	hamad to	1	2.0	2.0	21.6
	hamed to	1	2.0	2.0	23.5
	hidd	1	2.0	2.0	25.5
	hidya	1	2.0	2.0	27.5
	hoora	1	2.0	2.0	29.4
	indian	1	2.0	2.0	31.4
	isa	2	3.9	3.9	35.3
	isa n al	1	2.0	2.0	37.3
	isa town	1	2.0	2.0	39.2
	Isa town	1	2.0	2.0	41.2
	istiqlal	1	2.0	2.0	43.1
	jidhafs	3	5.9	5.9	49.0
	khawla	3	5.9	5.9	54.9
	Khawla	1	2.0	2.0	56.9
	mod kno	1	2.0	2.0	58.8
	muh	1	2.0	2.0	60.8
	muhrq	2	3.9	3.9	64.7
	noor	1	2.0	2.0	66.7
	pakistan	4	7.8	7.8	74.5
	s a aziz	1	2.0	2.0	76.5
	s.abdull	1	2.0	2.0	78.4
	saar	4	7.8	7.8	86.3
	saudi sc	1	2.0	2.0	88.2
	sitra	2	3.9	3.9	92.2
	w riffa	2	3.9	3.9	96.1
	wrifaa	1	2.0	2.0	98.0
	wriffa	1	2.0	2.0	100.0

Total	51	100.0	100.0	

area

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	hamad to	1	2.0	2.0	2.0
	Hamadtow	6	11.8	11.8	13.7
	isa town	1	2.0	2.0	15.7
	isatown	2	3.9	3.9	19.6
	Isatown	6	11.8	11.8	31.4
	IsaTown	1	2.0	2.0	33.3
	jidhafs	3	5.9	5.9	39.2
	Man	2	3.9	3.9	43.1
	Manama	11	21.6	21.6	64.7
	MAnama	1	2.0	2.0	66.7
	Muharaq	6	11.8	11.8	78.4
	saar	4	7.8	7.8	86.3
	saudi sc	1	2.0	2.0	88.2
	sitra	1	2.0	2.0	90.2
	Sitra	1	2.0	2.0	92.2
	w riffa	2	3.9	3.9	96.1
	wrifaa	1	2.0	2.0	98.0
	wriffa	1	2.0	2.0	100.0
	Total	51	100.0	100.0	

email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Home	25	49.0	50.0	50.0
	home/university	21	41.2	42.0	92.0
	university	4	7.8	8.0	100.0
	Total	50	98.0	100.0	
Missing		1	2.0		
Total		51	100.0		

facebook

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Home	31	60.8	72.1	72.1
	home/university	12	23.5	27.9	100.0
	Total	43	84.3	100.0	
Missing		8	15.7		
Total		51	100.0		

wikis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Home	8	15.7	66.7	66.7
	home/university	2	3.9	16.7	83.3
	university	2	3.9	16.7	100.0
	Total	12	23.5	100.0	
Missing	would not say	39	76.5		
Total		51	100.0		

skype

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Home	21	41.2	87.5	87.5
	university	3	5.9	12.5	100.0
	Total	24	47.1	100.0	
Missing	would not say	27	52.9		
Total		51	100.0		

hours_email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	i dont use it	4	7.8	7.8	7.8
	less than 1	25	49.0	49.0	56.9
	>=1 but<2	14	27.5	27.5	84.3
	>2	8	15.7	15.7	100.0
	Total	51	100.0	100.0	

hours_skype

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	i dont use it	29	56.9	56.9	56.9
	<1	12	23.5	23.5	80.4
	>=1 but<2	6	11.8	11.8	92.2
	>2	4	7.8	7.8	100.0
	Total	51	100.0	100.0	

hours_wikis

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	i dont use it	39	76.5	78.0	78.0
	<1	4	7.8	8.0	86.0
	>=1 but<2	5	9.8	10.0	96.0
	>2	2	3.9	4.0	100.0
	Total	50	98.0	100.0	
Missing		1	2.0		
Total		51	100.0		

hours_facebook

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	i dont use it	4	7.8	8.3	8.3
	<1	14	27.5	29.2	37.5
	>=1 but<2	16	31.4	33.3	70.8
	>2	14	27.5	29.2	100.0
	Total	48	94.1	100.0	
Missing		3	5.9		
Total		51	100.0		

Chapter 7

BAH

Independent Samples Test

	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	(2-tailed)	Mean Difference	d. Error Difference	Confidence Interval of the Difference	
								Lower	Upper
al variances assumed	5.158	.026	-1.836	66	.071	-.529	.288	-1.105	.046
al variances not assumed			-1.836	54.774	.072	-.529	.288	-1.107	.049

Group Statistics BAH

	categories	N	Mean	Std. Deviation	Std. Error Mean
phishing	acad	34	.0294	.17150	.02941
	othe	34	.0882	.28790	.04937
ignorance	acad	34	.0882	.28790	.04937
	othe	34	.3824	.65202	.11182
spam	acad	34	.0882	.28790	.04937
	othe	34	.4706	.74814	.12831

BAH

Independent Samples Test

		Levene's Test for Equality of Variances		T-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
phishing	Equal variances assumed	4.453	.039	-1.024	66	.310	-.05882	.05747	-.17357	.05592
	Equal variances not assumed			-1.024	53.800	.311	-.05882	.05747	-.17406	.05641
ignorance	Equal variances assumed	21.002	.000	-2.406	66	.019	-.29412	.12224	-.53817	-.05006
	Equal variances not assumed			-2.406	45.397	.020	-.29412	.12224	-.54026	-.04798
spam	Equal variances assumed	29.198	.000	-2.781	66	.007	-.38235	.13748	-.65684	-.10787

Equal variances not assumed			-2.781	42.564	.008	-.38235	.13748	-.65968	-.10502

BAH

Independent Samples Test

	Levene's Test for Equality of Variances		t-test for Equality of Means					
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference

									Lower	Upper
embededVAR00004	Equal variances assumed	2.039	.158	-.293	66	.770	-.05882	.20066	-.45945	.34181
	Equal variances not assumed			-.293	65.220	.770	-.05882	.20066	-.45954	.34190

UK

Group Statistics

	uk_group	N	Mean	Std. Deviation	Std. Error Mean
uk_freq	acad	18	2.17	2.728	.643
	other	17	1.71	1.687	.409

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
uk_freq	Equal variances assumed	.151	.700	.597	33	.555	.461	.772	-1.110	2.032
	Equal variances not assumed			.605	28.576	.550	.461	.762	-1.099	2.020

Independent Samples Test

	Levene's Test for Equality of Variances		t-test for Equality of Means					
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference

									Lower	Upper
uk_freq	Equal variances assumed	.151	.700	.597	33	.555	.461	.772	-1.110	2.032
	Equal variances not assumed			.605	28.576	.550	.461	.762	-1.099	2.020

“UK”Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
uk_freq	Equal variances assumed	.151	.700	.597	33	.555	.461	.772	-1.110	2.032
	Equal variances not assumed			.605	28.576	.550	.461	.762	-1.099	2.020

Group Statistics

	uk_group	N	Mean	Std. Deviation	Std. Error Mean
uk_ac_embe	acad	18	.9444	1.66176	.39168
	other	17	1.2941	1.61108	.39075
uk_ac_phis	acad	18	.2222	.64676	.15244
	other	17	.1176	.48507	.11765

uk_ac_spam	acad	18	.1111	.47140	.11111
	other	17	.2353	.56230	.13638
uk_RS	acad	18	.4444	.78382	.18475
	other	17	.8235	1.28624	.31196
uk_attc_IG	acad	18	.3889	1.41998	.33469
	other	17	.6471	1.16946	.28364
uk_RD	acad	18	.3333	1.02899	.24254
	other	17	.1765	.52859	.12820

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
uk_ac_embe	Equal variances assumed	1.573	.219	-.631	33	.532	-.34967	.55376	-1.47631	.77697
	Equal variances not assumed			-.632	32.974	.532	-.34967	.55326	-1.47532	.77597
uk_ac_phis	Equal variances assumed	1.202	.281	.539	33	.594	.10458	.19415	-.29043	.49959
	Equal variances not assumed			.543	31.433	.591	.10458	.19256	-.28794	.49709

uk_ac_spam	Equal variances assumed	1.659	.207	-.710	33	.483	-.12418	.17501	-.48024	.23187
	Equal variances not assumed			-.706	31.308	.485	-.12418	.17591	-.48281	.23444
uk_RS	Equal variances assumed	2.277	.141	-1.060	33	.297	-.37908	.35770	-1.10683	.34866
	Equal variances not assumed			-1.046	26.162	.305	-.37908	.36256	-1.12411	.36594
uk_attc_IG	Equal variances assumed	.427	.518	-.585	33	.562	-.25817	.44119	-1.15579	.63945
	Equal variances not assumed			-.588	32.420	.560	-.25817	.43871	-1.15134	.63500
uk_RD	Equal variances assumed	1.573	.219	.562	33	.578	.15686	.27908	-.41092	.72465
	Equal variances not assumed			.572	25.696	.572	.15686	.27433	-.40737	.72109

Group Statistics

	uk_group	N	Mean	Std. Deviation	Std. Error Mean
uk_ac_embe	acad	18	.9444	1.66176	.39168
	other	17	1.2941	1.61108	.39075
uk_ac_phis	acad	18	.2222	.64676	.15244
	other	17	.1176	.48507	.11765
uk_ac_spam	acad	18	.1111	.47140	.11111
	other	17	.2353	.56230	.13638
uk_RS	acad	18	.4444	.78382	.18475
	other	17	.8235	1.28624	.31196
uk_attc_IG	acad	18	.3889	1.41998	.33469

	other	17	.6471	1.16946	.28364
uk_RD	acad	18	.3333	1.02899	.24254
	other	17	.1765	.52859	.12820

Table 8.1 Mean and standard deviation values of total score shown according webmail type

	Email client	Mean	Std. Deviation	N
Security	yahoo	31.3333	3.50000	9
	Gmail	33.0968	4.30004	31
	Hotmail	31.8649	3.67546	37
	Gmail+Hotmail	30.8571	4.52101	14
	Total	32.0769	4.03383	91
Trust	yahoo	33.6667	3.50000	9
	Gmail	32.5806	5.26482	31
	Hotmail	32.5946	3.48377	37
	Gmail+Hotmail	32.2143	3.80644	14
	Total	32.6374	4.17271	91
usefulness	yahoo	23.1111	3.21887	9
	Gmail	24.6129	3.84428	31
	Hotmail	24.4865	3.21128	37
	Gmail+Hotmail	24.2857	4.25040	14
	Total	24.3626	3.57310	91
Ease	yahoo	20.6667	2.54951	9
	Gmail	21.4516	2.57991	31
	Hotmail	21.4865	2.10319	37
	Gmail+Hotmail	21.6429	3.43303	14
	Total	21.4176	2.51690	91

Table 8.2: Multivariate Results for Comparing Scores

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Wilks' Lambda	.014	1504.254[a]	4.000	84.000	.000
email_client	Wilks' Lambda	.873	.976	12.000	222.535	.473

Table 8.3: One Way ANOVA Results for Comparing Scores Given to Webmail Types on Each Security Dimension Taken Alone

So Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	Security	59.713[a]	3	19.904	1.233	.303
	t	12.209[b]	3	4.070	.228	.877
	ulness	16.689[c]	3	5.563	.427	.734
		5.997[d]	3	1.999	.308	.819
Intercept	security	66856.923	1	66856.923	4140.637	.000
	trust	71025.500	1	71025.500	3974.223	.000
	usefulness	38505.234	1	38505.234	2958.425	.000
	ease	30051.335	1	30051.335	4634.469	.000
ail clients	security	59.713	3	19.904	1.233	.303
	trust	12.209	3	4.070	.228	.877
dim1	usefulness	16.689	3	5.563	.427	.734
	ease	5.997	3	1.999	.308	.819
Error	security	1404.748	87	16.147		
	trust	1554.824	87	17.872		
Dim1	usefulness	1132.344	87	13.015		
	ease	564.135	87	6.484		
Total	security	95097.000	91			
	trust	98500.000	91			
Dim1	usefulness	55161.000	91			
	ease	42313.000	91			

Corrected Total		security	1464.462	90			
		trust	1567.033	90			
	Dim1						
		usefulness	1149.033	90			
		ease	570.132	90			

Appendix G

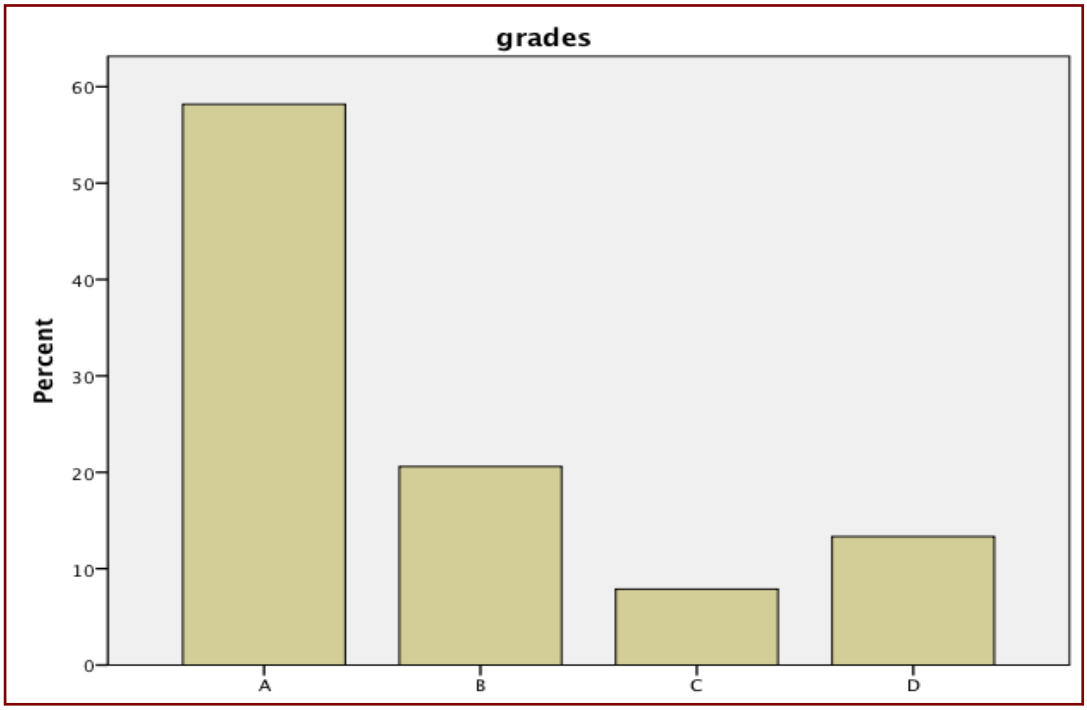
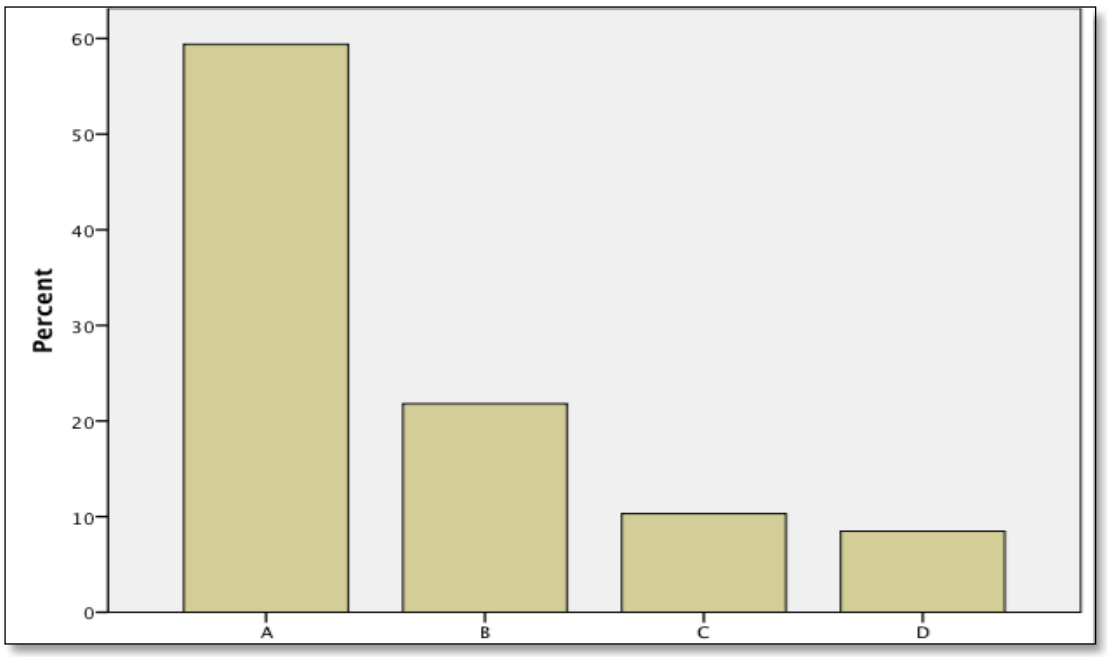
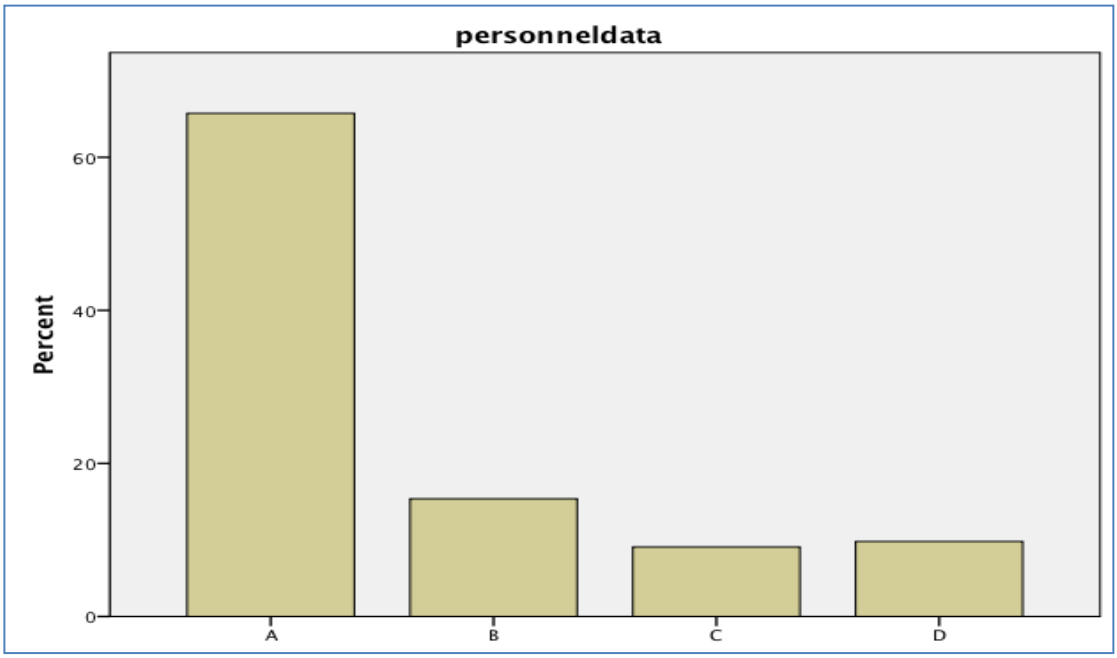


Figure 1: The respondent's preference towards grades privacy



The respondent's preference towards collaborative data privacy



The respondent's preference towards personal data privacy

Chapter 6-figures

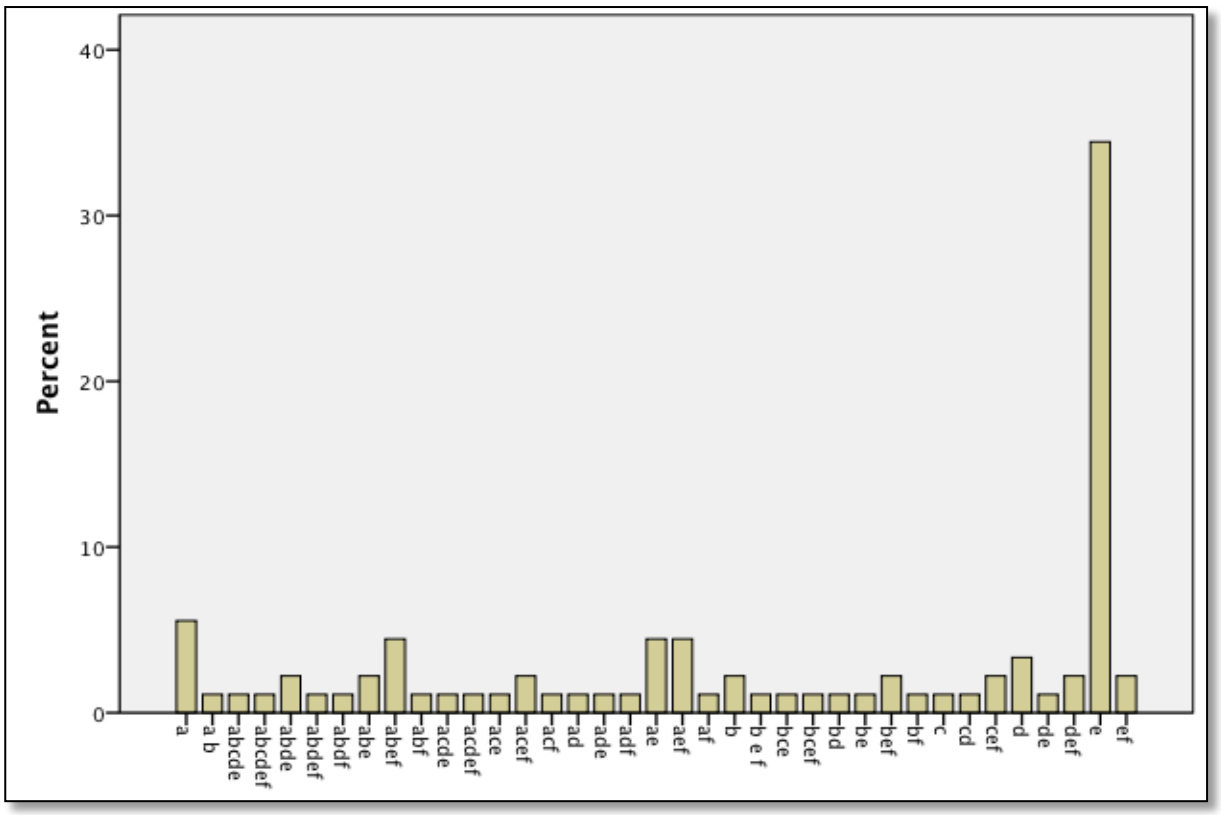


Figure 6.1: Frequency of perceptions about the security of email in general in Bahrain

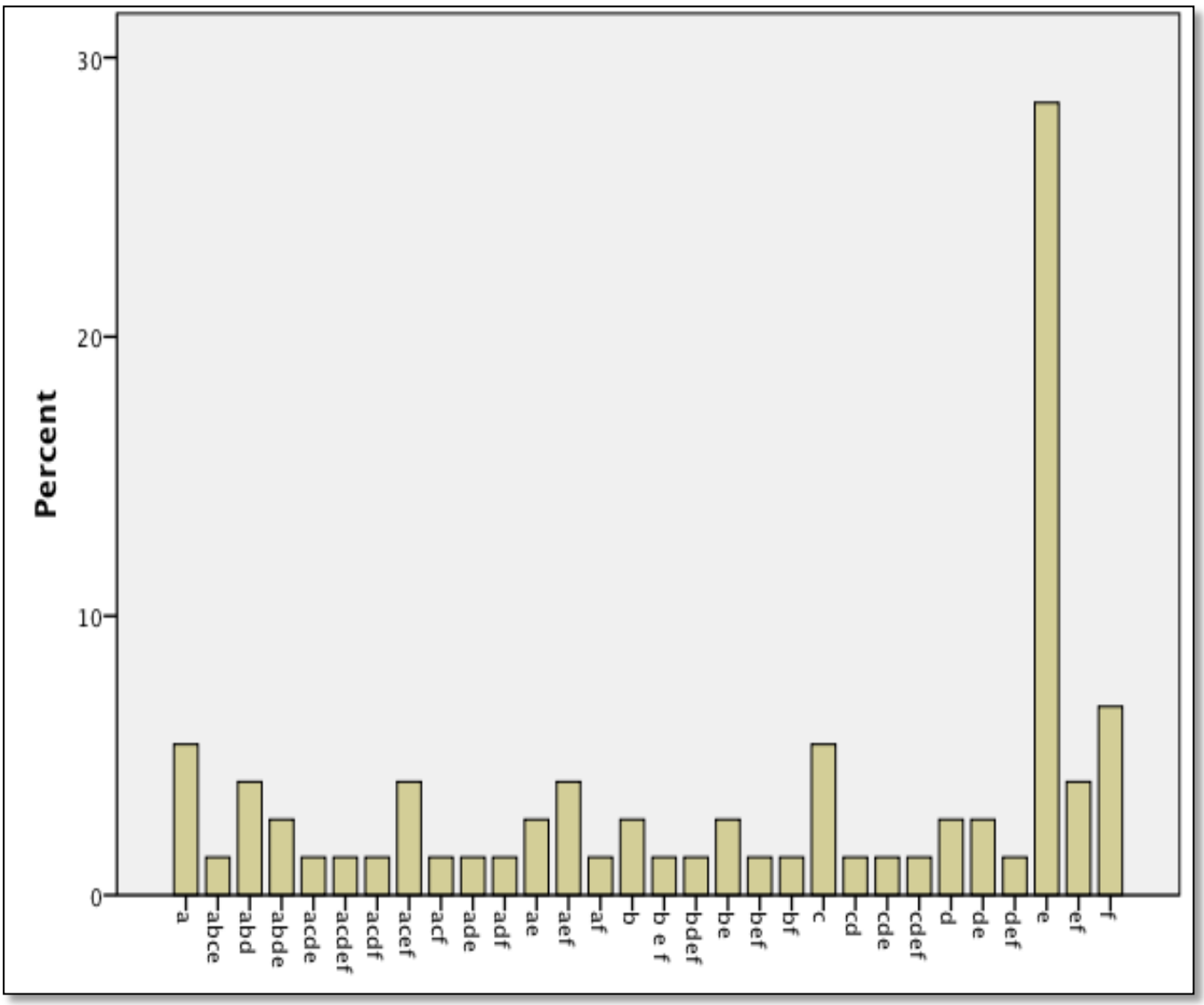


Figure 6.2: Frequency of perceptions about the security of the students' frequent email in Bahrain

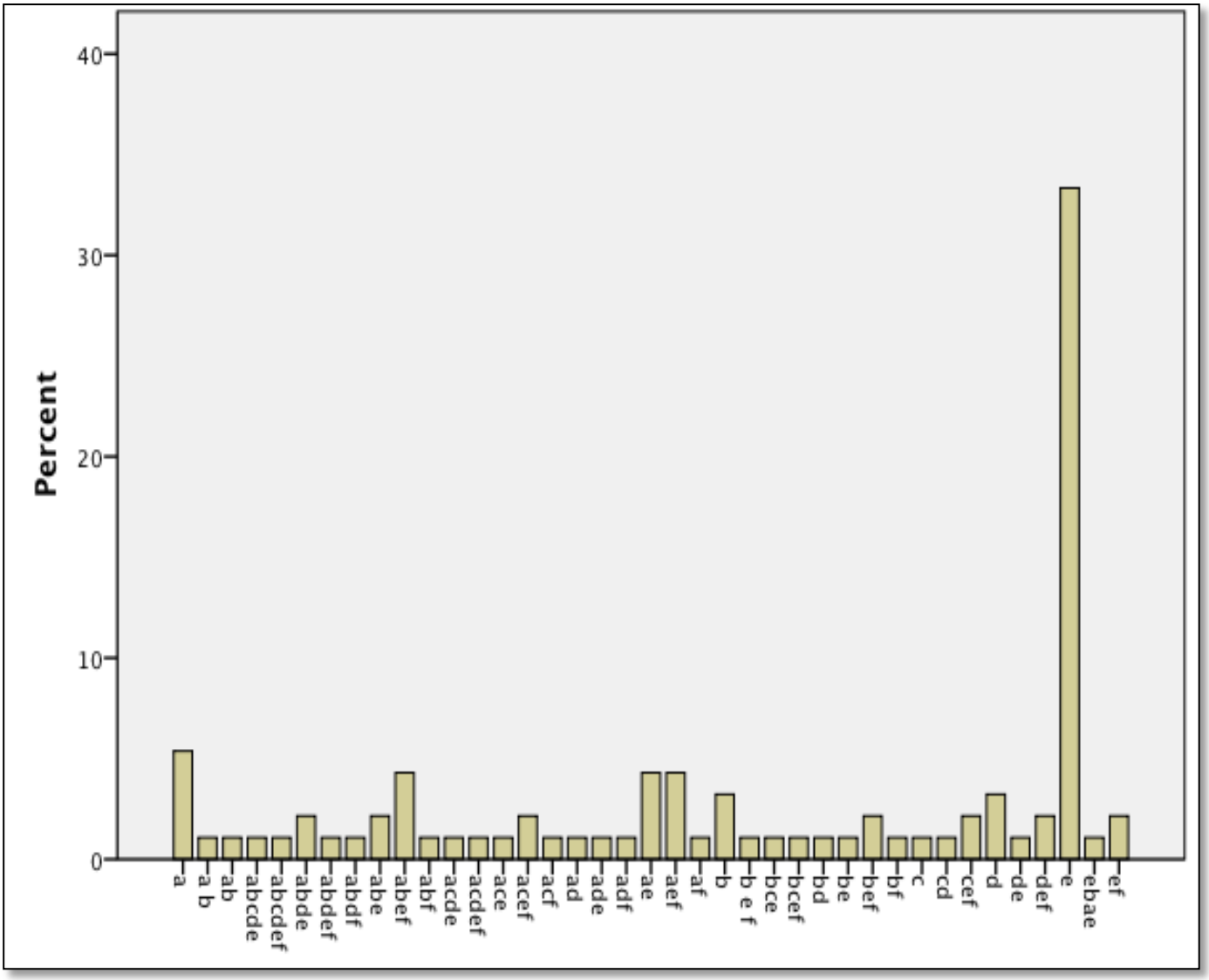


Figure 6.3 Frequency of perceptions about the security of email in general in the UK

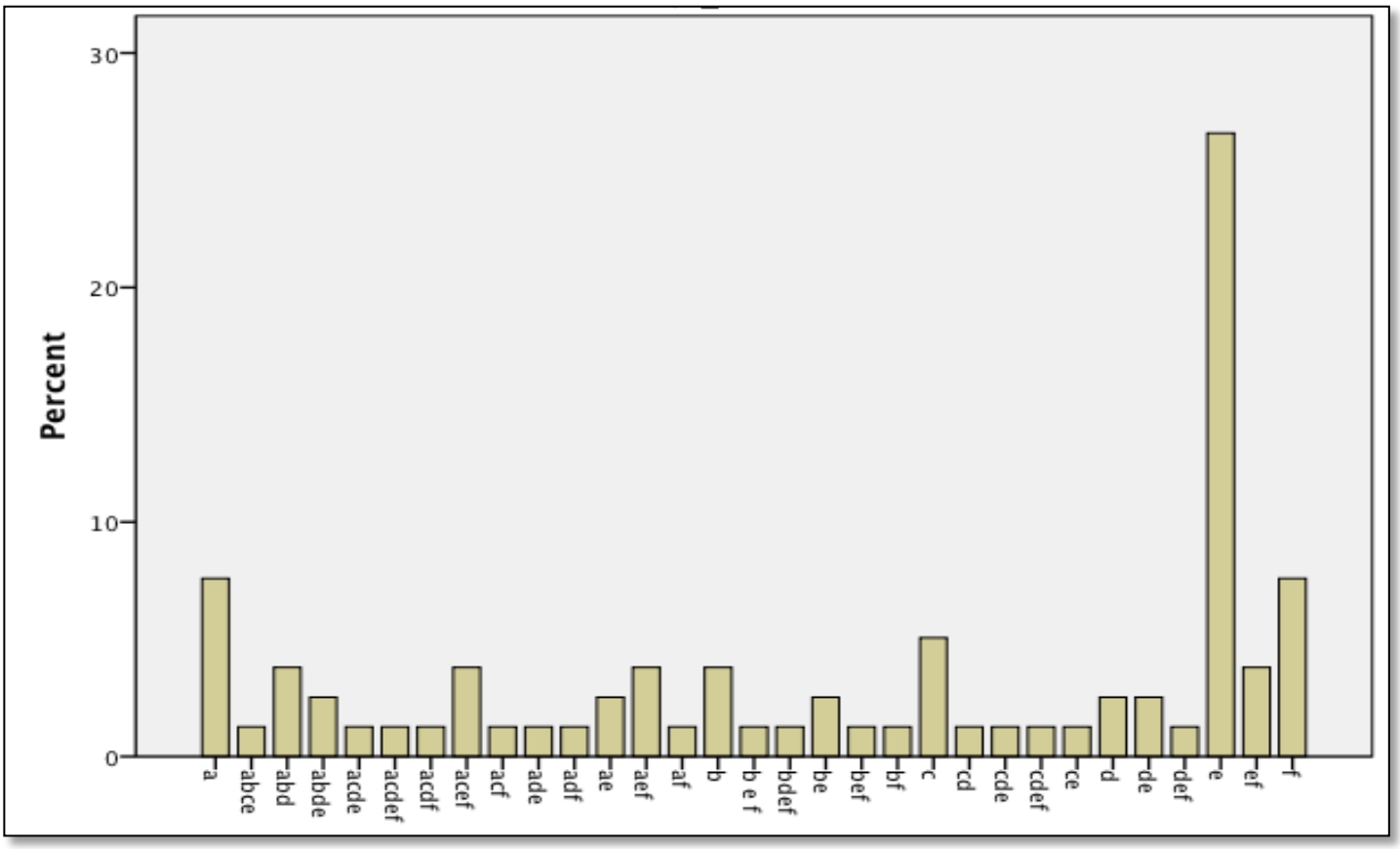


Figure 6.4: Frequency of conceptions about the security of students' frequent email in UK

The legend for items in this questionnaire-3 is shown in Table 6.3 below.

Table 6.3: Legend for the secure email perceptions of email

a	Supports encrypted information that can be read by your intended recipient
b	Is authorized with digital signature
c	Detects spoofing or phishing
d	Hasn't been corrupted during transmission.
e	If it has attachments, the attachments will have been scanned by anti-virus software
f	Has been filtered through anti-spam detectors